Surfing the third wave of computing : consumer contracting with eObjects in Australia

Author:
Manwaring, Kayleen

Publication Date:
2019

DOI:
https://doi.org/10.26190/unsworks/3892

Surfing the Third Wave of Computing: Consumer Contracting with eObjects in Australia

Kayleen Elizabeth Manwaring

A Dissertation in fulfilment
of the requirements for the Degree of
Doctor of Philosophy

Faculty of Law

November 2019

UNSW SYDNEY | Australia's Global University

Thesis/Dissertation Sheet

Surname/Family Name	:	**Manwaring**
Given Name/s	:	**Kayleen**
Abbreviation for degree as give in the University calendar	:	**PhD**
Faculty	:	**Law**
School	:	**Law**
Thesis Title	:	**Surfing the Third Wave of Computing: Consumer Contracting with eObjects in Australia**

Abstract 350 words maximum: (PLEASE TYPE)

A 'third wave' of computing is emerging, based on widespread use of processors with data handling and communications capabilities embedded in a variety of objects and environments not previously computerised, such as refrigerators, buildings, cars, fitness trackers and hairbrushes. With the ensuing sociotechnical change the possibility arises of a 'regulatory disconnection' between current consumer protection law and new things, activities and relationships brought about by the third wave.

This third wave has had many names, including ubiquitous and pervasive computing, ambient intelligence and the Internet of Things. However, significant definitional inconsistencies and incoherencies exist, necessitating the development in this dissertation of a technical research framework. This framework involves abstracting and analysing the attributes of, and interactions among, the technologies, and defining a unifying concept for the central technological element, the 'eObject'.

The dissertation proceeds to outline the categories of legal problems that can arise in the context of sociotechnical change, emphasising that not every instance of sociotechnical change operates outside the scope of existing legal rules. Therefore, new things, activities and relationships enabled by new technologies should first be judged against existing rules and their goals.

The attributes and interactions of eObjects are then interrogated to identify where sociotechnical change associated with eObjects might lead to challenges for consumers. The challenges identified are ones whose outcomes are in conflict with the goals of Australian consumer protection law, potentially giving rise to legal problems.

One of those identified challenges is examined in depth. Widespread digitisation of commerce has arguably given firms an enhanced ability not only to compile detailed customer profiles, but also to exploit consumers' individual biases and vulnerabilities. This dissertation argues that 0pportunities for such 'digital consumer manipulation' will be substantially increased by the widespread use of eObjects.

Provisions of the Australian Consumer Law (ACL) and related cases are examined to evaluate the effectiveness of Australian consumer protection law in the face of 'digital consumer manipulation' facilitated by eObjects. Legal problems with the ACL are identified; and some mechanisms for reconnection of consumer law with its goals and purposes are outlined and analysed. This examination allows for a 'reflecting back' on the utility of particular concepts and frameworks used in law and technology research.

Copyright Statement

Signed

Date .....9 December 2019.....

Authenticity Statement

I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis. No emendation of content has occurred and if there are any minor variations in formatting, they are the result of the conversion to digital format.

Signed

Date .....9 December 2019.....

Originality Statement

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the dissertation. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the dissertation. I also declare that the intellectual content of this dissertation is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Signed

Date …9 December 2019……

Inclusion of Publications Statement

UNSW is supportive of candidates publishing their research results during their candidature as detailed in the UNSW Thesis Examination Procedure.

Publications can be used in their thesis in lieu of a Chapter if:

- The student contributed greater than 50% of the content in the publication and is the "primary author", ie. the student was responsible primarily for the planning, execution and preparation of the work for publication
- The student has approval to include the publication in their thesis in lieu of a Chapter from their supervisor and Postgraduate Coordinator.
- The publication is not subject to any obligations or contractual agreements with a third party that would constrain its inclusion in the thesis

Please indicate whether this thesis contains published material or not.

☐ *This thesis contains no publications, either published or submitted for publication*

☒ *Some of the work described in this thesis has been published and it has been documented in the relevant Chapters with acknowledgement*

☐ *This thesis has publications (either published or submitted for publication) incorporated into it in lieu of a chapter and the details are presented below*

CANDIDATE'S DECLARATION

I declare that:

- I have complied with the Thesis Examination Procedure
- where I have used a publication in lieu of a Chapter, the listed publication(s) below meet(s) the requirements to be included in the thesis.

Name	**Signature**	**Date**
Kayleen Manwaring		9/12/2019

Publications Arising from this Dissertation

Peer-reviewed publications

Manwaring K, 'Surfing the Third Wave of Computing: Contracting with eObjects' (Proceedings DCIT 2016, Doctoral Consortium on Internet of Things, First International Conference on Internet of Things and Big Data 2016, Rome, 22–25 April 2016) 3–13

—— 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 Deakin Law Review 53–84 (post print available online 1 September 2016)

—— 'Emerging Information Technologies: Challenges for Consumers' (2017) 17(2) *Oxford University Commonwealth Law Journal* 265–89 (published online 17 August 2017)

—— 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (2018) 26(2) *Competition and Consumer Law Journal* 141 (published online 3 December 2018)

Manwaring K and Clarke R, 'Surfing the Third Wave of Computing: A Framework for Research into eObjects' (2015) 31 Computer Law & Security Review 586–603[1] (published online 28 August 2015)

Other publications

Manwaring K, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (UNSW Law Research Paper No 2016–15, 2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690024>[2]

---

[1] Note that, as stated in the article's acknowledgements, the author of this dissertation undertook all substantial research and drafting for this article, while the co-author and PhD supervisor Professor Roger Clarke assisted with conception and structure, as well as critical review. As the content of this article was far more closely associated with the computer science and information systems disciplines than any legal discipline, attribution of co-authorship for this article followed authorship conventions in the computer science and information systems disciplines. The inclusion of material from this article in this dissertation was approved by UNSW Law's then Director of Postgraduate Research, Professor Gary Edmond, and the UNSW Law Annual Progress Review Panel assigned to this doctoral study.

[2] This research paper was subsequently extensively revised and published as Kayleen Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 Deakin Law Review 51. The initial research paper is nevertheless included as a separate publication in this dissertation because the published article omitted some material from the research paper that has been

——— 'Six Things Every Consumer Should Know About the Internet of Things' (*The Conversation*, 8 June 2017) <https://theconversation.com/six-things-every-consumer-should-know-about-the-internet-of-things-78765>

Open access to publications

According to UNSW's Open Access Policy, UNSW is committed to enabling Open Access to research outputs produced at UNSW and supports Australian Government Open Access initiatives to improve access to publicly funded scholarly information. Note that all of these publications, in working paper, pre-print, and/or post-print form, have been distributed open access on various academic websites, including via unsworks.unsw.edu.au, SSRN.com, researchgate.net, academia.edu, theconversation.com, rogerclarke.com, kayleenmanwaring.wordpress.com, and government websites including ntia.gov, humanrights.gov.au and accc.gov.au. This may mean that they have been further distributed via other websites by third parties without the control of the author of this dissertation.

used in this dissertation. The research paper has also been separately cited by other scholars.

ABSTRACT

A ‘third wave’ of computing is emerging, based on widespread use of processors with data handling and communications capabilities embedded in a variety of objects and environments not previously computerised, such as refrigerators, buildings, cars, fitness trackers and hairbrushes. With the ensuing sociotechnical change the possibility arises of a ‘regulatory disconnection’ between current consumer protection law and new things, activities and relationships brought about by the third wave.

This third wave has had many names, including ubiquitous and pervasive computing, ambient intelligence and the Internet of Things. However, significant definitional inconsistencies and incoherencies exist, necessitating the development in this dissertation of a technical research framework. This framework involves abstracting and analysing the attributes of, and interactions among, the technologies, and defining a unifying concept for the central technological element, the ‘eObject’.

The dissertation proceeds to outline the categories of legal problems that can arise in the context of sociotechnical change, emphasising that not every instance of sociotechnical change operates outside the scope of existing legal rules. Therefore, new things, activities and relationships enabled by new technologies should first be judged against existing rules and their goals.

The attributes and interactions of eObjects are then interrogated to identify where sociotechnical change associated with eObjects might lead to challenges for consumers. The challenges identified are ones whose outcomes are in conflict with the goals of Australian consumer protection law, potentially giving rise to legal problems.

One of those identified challenges is examined in depth. Widespread digitisation of commerce has arguably given firms an enhanced ability not only to compile detailed customer profiles, but also to exploit consumers’ individual biases and vulnerabilities. This dissertation argues that opportunities for such ‘digital consumer manipulation’ will be substantially increased by the widespread use of eObjects.

Provisions of the Australian Consumer Law (ACL) and related cases are examined to evaluate the effectiveness of Australian consumer protection law in the face of 'digital consumer manipulation' facilitated by eObjects. Legal problems with the ACL are identified; and some mechanisms for reconnection of consumer law with its goals and purposes are outlined and analysed. This examination allows for a 'reflecting back' on the utility of particular concepts and frameworks used in law and technology research.

ACKNOWLEDGEMENTS

Firstly, my deepest thanks to my amazing supervisors, Lyria Bennett Moses, Roger Clarke and Leon Trakman.

Also thanks to my panel and other colleagues at UNSW Law who were so generous with their comments and encouragement, particularly Alana Maurushat, Colin Picker, Prue Vines, Simon Halliday, Greg Weeks, Graham Greenleaf, and Directors of Postgraduate Research Theunis Roux, Gary Edmond, Sarah Williams and Rosemary Rayfuse. And of course thousands of extra thanks to Jenny Jarrett, who has held the hands of literally hundreds of us through this laborious process.

I literally could not have done this dissertation without the tremendous support of all of my current and former colleagues at the School of Taxation and Business Law and in the wider Business School. Particular thanks go to my mentor and friend, Fiona Martin, who would have physically pushed me over the line if she could, my Heads of School, John Taylor and Michael Walpole, and our School Manager, Maree Magafas.

Thanks also to those outside of UNSW who were so generous with their comments and ideas, particularly Gail Pearson and participants in the 2012 Sensor Society Conference, the 2017 Law Technology and Innovation Junior Scholars Forum, the 2017 Future of the Internet Conference, and the 2018 British and Irish Law Education and Technology Association Conference.

Many thanks to the staff of the Learning Centre and the Graduate Research School for organising the UNSW Thesis Bootcamps and for giving up their weekends to provide us with shelter, advice and Minties, particularly Pam Mort and Bianca Azar.

Much gratitude to all of those beautiful fellow travellers who provided me with advice, congratulations, solace and virtual hugs via the Facebook support groups PhD and Early Career Researchers, Older Wiser Learners (OWLs), Women in Academia and Women in Academia Australia.

Thanks also to my editors: Lilla Wendoloski, Marie-Louise Taylor, Matthew Blake and Capstone Editing.

Thanks to my family and friends for listening to me talk about my PhD for so many years, particularly the wonderful Fiona Henderson. Special mention to my sister Narelle (because she is awesome and demanded to be included).

Thanks to my mum, who gave up so much for my education. Also to my wonderful daughters, Kalila and Persia, who were so patient with Mummy's frequent absences throughout the whole process – and thanks for keeping me going with laughter and hugs. And to Stu – there are no words for the gifts of time and space you have given me. So I can only say a manifestly inadequate thank you for the nappy changes, 3 am wake-ups, lunches, pick-ups and drop-offs, school lunches, dinners (and democracy sausages), dishwashers stacked, school uniforms, Easter hats, solo evenings and weekends, nightmares consoled, Tae Kwon Do lessons and gradings, hair brushed, parent/teacher interviews attended, forms filled in, bills paid, storage acquired, wild gardens fought and subdued, and all the other emotional and physical labour you took on for me.

Finally, this dissertation is dedicated to Dad, Orana and Paul. I wish you were here.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AAT	Administrative Appeals Tribunal
ACCAN	Australian Communications Consumer Action Network
ACCC	Australian Competition and Consumer Commission
ACL	Australian Consumer Law
ACMA	Australian Communications and Media Authority
ACOLA	Australian Council of Learned Academies
AFSLs	Australian financial service licensees
APPs	Australian Privacy Principles
AUP	Acceptable Use Policy
CAANZ	Consumer Affairs Australian and New Zealand
CCA	Competition and Consumer Act 2010 (Cth)
CPRC	Consumer Policy Research Centre (Victoria)
CRA	Contracts Review Act 1980 (NSW)
DDOS	distributed denial of service
DOS	denial of service
EDPS	European Data Protection Supervisor
EPC	Electronic Product Code
EU	European Union
EULA	End User Licence Agreement
FCC	Federal Communications Commission (US)
FTC	Federal Trade Commission (US)
GSM	Global System for Mobile Communications
HaaS	hacking as a service
HRC	Human Rights Commission (Australia)

iHCI	implicit human-computer interaction
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
ISO	International Standards Organisation
ISP	Internet service provider
ITU	International Telecommunications Union
MAC	media access control
NSW	New South Wales
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
RFID	radio-frequency identification
SIM	Subscriber Identity/Identification Module
TPA	Trade Practices Act 1974 (Cth)
TPM	technological protection measure
TOU	Terms of Use
UCITA	Uniform Computer and Information Transactions Act (US model law)
UK	United Kingdom
UN	United Nations
US	United States of America
USDC	United States Department of Commerce
WIPO	World Intellectual Property Organization

LIST OF FIGURES

LIST OF TABLES

Cases

Australian Legislation and Instruments

European Legislation and Instruments

United States Legislation and Instruments

International Treaties and Instruments

Chapter 1 – The enquiry[3]

[3] Some parts of this chapter reproduce significant parts of a peer-reviewed conference paper published during the course of this doctoral study: Kayleen Manwaring, 'Surfing the Third Wave of Computing: Contracting with eObjects' (Proceedings DCIT 2016: First International Conference on Internet of Things and Big Data 2016, Rome, 22–25 April 2016).

1 INTRODUCTION

1.1 The 'third wave' in context

During the last two decades, a 'third wave of computing'[4] has emerged. This third wave amounts to a move away from a model of accessing the Internet and other internetworks[5] almost exclusively via a desktop computer and towards alternative forms of distributed information technologies, such as smartphones, wearable computers, and sensors and microprocessors embedded in everyday objects. The first wave of computing comprised the introduction of mainframe computing, with a 'many people to one machine' model. The second wave brought about personal computing, establishing the development of one-to-one relationships between people and their

[4] Mark Weiser, 'Ubiquitous Computing' (1996) <www.ubiq.com/hypertext/weiser/UbiHome.html> accessed 10 February 2018. This website is now no longer available, but the text is currently available at <https://web.archive.org/web/20180426170841/www.ubiq.com/weiser/UbiHome.html>.

[5] An internetwork is 'a collection of computer networks interconnected by routers and other devices so as to function as a single network', Susan Butler (ed), *Macquarie Dictionary: Australia's National Dictionary Online* (Macquarie Library 2003). The Internet is the largest – but not the only – example of an internetwork. The Internet is distinguished from other internetworks by its use of the Internet Protocol Suite for its communications, most notably the TCP and IP protocols: Roger Clarke, 'Origins and Nature of the Internet in Australia' (*Xamax Consultancy,* 29 January 2004) <www.rogerclarke.com/II/OzI04.html> accessed 13 May 2015.

computers. The third wave envisages a move to a 'many people to many machines' model.[6]

Mobile commerce is now unremarkable. It forms part of the mainstream of e-commerce technologies, with applications for mobile entertainment, retail shopping, banking, stock trading and gambling all well established.[7] What is rapidly emerging is the use of computing devices embedded into buildings and everyday objects. Current applications include home[8] and industrial[9] automation, driverless vehicles,[10] consumer products such as fitness trackers[11] and Internet-connected toys,[12] energy management,[13] healthcare,[14] and

[6] Mark Weiser and John Seely Brown, 'The Coming Age of Calm Technology' in Peter J Denning and Robert Metcalfe (eds), *Beyond Calculation: The Next 50 Years of Computing* (Springer 1997) 76–78.

[7] Efraim Turban and others, *Electronic Commerce: A Managerial and Social Networks Perspective* (8th edn, Springer 2015) 262-264.

[8] For example, Internet-enabled light, energy, security, entertainment, appliances and water: ibid 314–15.

[9] For example, wireless sensor networking products such as SmartMesh WirelessHART: Analog Devices, 'SmartMesh WirelessHART' <www.linear.com/products/smartmesh_wirelesshart> accessed 9 September 2018.

[10] For example, Daimler 'Smart' brand cars, Google's driverless car and SARTRE self-driven road trains. See Turban and others, *Electronic Commerce 2012: A Managerial and Social Networks Perspective* (Global Edn, Pearson Education 2012) 315–16.

[11] For example, Fitbit: Mahmudur Rahman, Bogdan Carbunar and Madhusudan Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) arXiv:13045672 [csCR]; Mario Ballano Barcena, Candid Wueest and Hon Lau, *How Safe is Your Quantified Self?* (Symantec Security Response Report, 11 August 2014).

[12] For example, Security Ledger, 'Update: Hello Barbie Fails Another Security Test' (*Security Ledger,* 4 December 2015) <https://securityledger.com/2015/12/hello-barbie-fails-another-security-test/> accessed 17 December 2015.

[13] For example, the Smart Grid, Smart City trials in New South Wales: see Australia, Department of Industry Innovation and Science, 'Smart Grid, Smart City' <http://webarchive.nla.gov.au/gov/20160615043539/http://www.industry.gov.au/Energy/Programmes/SmartGridSmartCity/Pages/default.aspx> accessed 9 September 2018; and similar trials in the US (see United States, Department of Energy, Office of Electricity Delivery and Energy Reliability, 'Smartgrid.gov' <www.smartgrid.gov> accessed 9 September 2018); and in the EU (European Commission, Joint Research Centre, Smart Electricity Systems and Interoperability, 'Smart Grid Projects Outlook 2017' <https://ses.jrc.ec.europa.eu/smart-grids-observatory> accessed 9 September 2018).

[14] For example, AliveCor EKG monitor, 6SensorLabs Nima gluten tester, Nokia BPM+ wireless blood pressure monitor and iHealth Lab Inc Wireless Smart Gluco-Monitoring System: Meeroona, '17 Portable Health Gadgets That Can Change Your

environmental monitoring,[15] to name just a few. Technological developments have resulted in significant sociotechnical change:[16] that is, the creation of new things to be bought and sold, new activities for business and consumers to engage in, and new kinds of commercial relationships between consumers and businesses.[17] These developments have also resulted in a change in the attributes and activities of consumers.

It is widely recognised that sociotechnical change often gives rise to distinct legal problems.[18] If the introduction of new or significantly modified forms or affordances of information technology give rise to inconsistencies, unmet expectations and unpredictable outcomes in the law, this may well lead to substantial problems for those using or interacting with the technologies, as well as those who provide products and services relating to the technologies. The aim of this dissertation is to examine whether aspects of contract and consumer protection law in Australia, specifically as they apply to the supply and use of 'third wave' technologies in consumer transactions, protects the interests of consumers in line with the goals of Australia's consumer protection laws.

1.2 Aims and structure of chapter

In **section 2**, this chapter introduces and provides a brief description of the technology that is the subject of this dissertation, as a prelude to a more detailed discussion in **Chapter 2. Section 3** sets out the general and specific

Life' (*Travel Away,* 13 November 2018) <https://travelaway.me/portable-health-gadgets/> accessed 22 December 2018.

[15] Luís M Oliveira and Joel J Rodrigues, 'Wireless Sensor Networks: A Survey on Environmental Monitoring' (2011) 6 Journal of Communications 143.

[16] The meaning of 'sociotechnical change' is discussed in more detail in **section 2.2.1.1** of **Chapter 3**.

[17] For some examples of this, see Turban and others, *Electronic Commerce: A Managerial and Social Networks Perspective* (n 7) ch 6.

[18] See for example, Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer 2011); Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (OUP 2008); Lyria Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 2 University of Illinois Journal of Law, Technology & Policy 239.

research questions that are the subject of the enquiry and defines key terms. **Section 4** outlines the significance and contribution of the research project. **Section 5** describes the approach to research undertaken during the course of doctoral study, necessary exclusions from the scope of this dissertation, and the currency of the research. Finally, **section 6** sets out the structure of the dissertation, and the subject of each chapter.

2 EOBJECTS: THE TECHNOLOGY AT ISSUE

Despite the fact that it is easy to point to current (and potential) examples of third wave technologies, it is difficult to define the scope of the third wave both accurately and usefully. The terminology used by researchers, industry participants and governments is not fixed, and a number of different terms are frequently used. The most dominant terms in the literature are **ubiquitous computing**,[19] **pervasive computing**,[20] **ambient intelligence**,[21] and the **Internet of Things**[22] (**IoT**). These terms are sometimes used interchangeably in the literature. Other times they are used in different but overlapping contexts or with a wider or narrower scope of meaning. Profusion and confusion of terms abound and terms and descriptions in the literature appear to be contingent on a number of factors. They vary over geographical locations and with individual researchers, and they change over time.

Therefore, as one of the initial steps to achieving the objective of this dissertation, **Chapter 2** outlines the literature on historical and current definitions of third wave technologies. In particular, **Chapter 2** discusses the dominant terms set out above in order to provide a clear statement of the

[19] For example, Mark Weiser, 'The Computer for the 21st Century' (1991) Scientific American 94. See discussion in **section 3.1** of **Chapter 2**.

[20] For example, Frank Adelstein and others, *Fundamentals of Mobile and Pervasive Computing* (McGraw-Hill 2005). See discussion in **section 3.1** of **Chapter 2**.

[21] For example, Information Society and Technology Advisory Group, *Strategic Orientations and Priorities for IST in FP6* (Report, European Commission, June 2002). See discussion in **section 3.3** of **Chapter 2**.

[22] For example, Neil Gershenfeld, Raffi Krikorian and Danny Cohen, 'The Internet of Things' (2004) Scientific American 76. See discussion in **section 3.4** of **Chapter 2**.

terminology and concepts behind the new model. After tracing the history of these terms and their various uses, **Chapter 2** goes on to extract and analyse the key attributes of the terms. To overcome the problems of scope definition and conflicting terms, in **Chapter 2** this dissertation proposes a new term, 'eObject', for the central technological element of the new model, and defines that term as follows:

> An eObject is an object that is not inherently computerised, but into which has been embedded one or more computer processors with data collection, data handling and data communication capabilities.

However, while this definition outlines the core attributes of the new model, by itself it does not give a full picture of the types of technologies that the literature discusses. Therefore, **Chapter 2** proceeds to outline a research framework of core and other attributes to assist in exploring legal problems that might arise out of sociotechnical change brought about by eObjects.

As stated above, there are myriad terms used in the literature for this wave of technological development. **Chapter 2** discusses the most important terms in detail along with the differences, and similarities, among them. However, except in the discussion in **Chapter 2**, this dissertation uses the term 'eObjects' even when referencing literature that employs a different term, unless a direct quotation is given, or the nature of the precise term employed is material to the relevant discussion. Note that 'eObjects' is not given a leading capital when the term is used to begin a sentence, for the sake of readability.

3 RESEARCH QUESTIONS

3.1 General research questions

The dissertation examines sociotechnical change brought about by eObjects and the systems in which they participate. It assesses the extent to which this change could give rise to legal problems in the context of the protection of consumers entering into contracts for the supply of, or mediated by, eObjects.

In particular, the aim of this dissertation is to answer the following general research questions:

1) What types of sociotechnical change brought about by eObjects and the systems in which they participate will affect consumers?

2) To what extent do those types of sociotechnical change have the potential to hinder achievement of the goals of consumer protection law in Australia?

3) To what extent is there a gap between existing consumer protection laws and the goals they were intended to achieve in the context of the phenomenon of 'digital consumer manipulation' in which eObjects and related systems are involved in data collection and/or mediation of marketing messages?

3.2 Specific research questions

In order to answer the broad questions set out in **section 3.1** of this chapter, this dissertation investigates and proposes answers to the following specific questions:

1) What are the main attributes of the technologies underlying the emerging 'third wave' of computing? (**Chapter 2**)

2) What conceptual framework is appropriate for investigating legal problems arising out of sociotechnical change brought about by eObjects and the systems in which they participate? (**Chapter 3)**

3) What goals of Australia's contract and consumer protection law are relevant to the development, sale and use of eObjects? (**Chapter 3**)

4) What types of sociotechnical change could the attributes of eObjects give rise to that could be relevant to consumers? (**Chapters 4, 5 and 6**)

5) What challenges for consumers are likely to arise in relation to the types of sociotechnical change identified in Q(4)? (**Chapter 5**)

6) Of the challenges identified in Q(5), which of these have detrimental outcomes that are likely to conflict with the goals of Australian consumer protection law? (**Chapter 5**)

7) What legal problems arise out of digital consumer manipulation enabled by eObjects? (**Chapter 6**)

8) Why is it important to examine the legal problems identified in Q(7)? (**Chapter 6**)

9) What are the implications of the legal problems identified in Q(7)? (**Chapters 6**, **7** and **8**)

10) In light of the issues identified in this dissertation, what modifications to the conceptual framework could improve its utility for the purposes of this dissertation and support further research into sociotechnical change and law? (**Chapters 3** and **8**)

3.3 A broad and deep approach

This enquiry combines a broad approach to establishing general areas of concern around the consumer protection implications of eObjects and associated systems with an in-depth analysis of one of those implications. It begins with a wide-ranging examination of the nature of eObjects, the types of sociotechnical change they bring about, and a high-level identification of the issues and challenges to which they give rise. This initial broad examination is important to lay proper foundations for the subsequent deeper analysis of actual legal problems arising out of the advent of eObjects.

The breadth element of the enquiry is revealed in the investigation of the general research **Questions 1** and **2** set out in **section 3.1** of this chapter. Researching the answer to **Question 1** requires a high-level analysis of the sociotechnical change enabled by eObjects and related systems. As discussed in **Chapter 2**, this analysis is undertaken to outline a technical research framework for analysing the implications of the 'third wave' from a range of perspectives, including the legal. This technical research framework is used to underpin analysis of the consumer challenges arising out of this

sociotechnical change, in order to answer **Question 2**. The research and analysis undertaken for **Question 2** identify whether likely detrimental outcomes for consumers faced with these challenges may conflict with the goals of Australian consumer protection law.

However, this broad mapping of challenges against goals does not and cannot reveal *specific* legal problems, just the potential for them. What it can and does do is lay an essential foundation for the next step: a deep doctrinal analysis of cases and legislation to assess whether Australia's consumer protection law is adequate to address the supply to and use of eObjects by consumers.

To undertake and complete a detailed doctrinal analysis for *all* of the challenges identified in **Chapter 5** would be impossible within the scope of this dissertation. Therefore, the scope of the general research **Question 3** is narrowed to an in-depth analysis of only one of the challenges identified, that of digital consumer manipulation. The extensive analysis of cases and legislation set out in **Chapter 6** establishes the existence of specific legal problems arising out of digital consumer manipulation.

The broad identification of conflicting challenges, and the in-depth doctrinal analysis of digital consumer manipulation, have an additional function in this dissertation over and above the practical purposes set out above. In 2007, Cockfield and Pridmore expressed the hope that newly developing law and technology theory could 'reflect back' on doctrinal analysis of particular areas of law, to provide a 'broader perspective' which would better inform legal analysis.[23] However, this process of 'reflecting back' is not one-way. The examination of both breadth and depth in this study provides insights into the usefulness and applicability of a particular general conceptual framework and approach to law and technology research set out in **Chapter 3.** These insights are discussed in **section 3** of **Chapter 3** and **section 2.2** of **Chapter 8**.

[23] Arthur J Cockfield and Jason Pridmore, 'A Synthetic Theory of Law and Technology' (2007) 8 Minnesota Journal of Law, Science & Technology 475, 496.

For example, the approach set out in **section 3** of **Chapter 3** requires the identification of the goals and purposes of existing law that may apply to a particular type of sociotechnical change. The recent consolidation of the Australian Consumer Law (**ACL**)[24] into one national law has resulted in a statement of some relatively (although not perfectly) clear goals and objectives (set out in **section 4** of **Chapter 3**). The existence of such a readily available list of goals and objectives is by no means universal in Australian law, and shortens the time needed to make it a good initial case study for a practical and informed perspective on general conceptual approaches to law and technology research**.** The examination of the particular challenge chosen for detailed analysis (that is, digital consumer manipulation enabled by eObjects) is also helpful for this objective. The nature of digital consumer manipulation allows for the contrasting of different provisions of the ACL, some of which are 'technologically neutral' and others of which are 'technologically specific'.

3.4 Some key definitions

To understand the research questions fully, some key terms need to be defined, in particular 'eObjects', 'consumer', 'sociotechnical change', 'legal problems' and 'digital consumer manipulation'. **Section 2** of this chapter provided a preliminary definition of eObjects, and a fuller definition is provided in **Chapter 2**. Definitions of 'sociotechnical change' and 'legal problems' are interrogated as part of the conceptual framework in **Chapter 3**, in **sections 2.2.1.1** and **2.2.1.2** respectively**.** The nature of 'digital consumer manipulation' is explored extensively in **section 3.3.1** of **Chapter 5** and throughout **Chapter 6**. However, it is worthwhile at this stage of the dissertation to discuss the meaning of 'consumer' in this dissertation, as a generally accepted and precise definition of the word does not exist.[25]

[24] Contained in Competition and Consumer Act 2010 (Cth) (**CCA**) sch 2.

[25] Trish O'Sullivan, 'The Definition of "Consumer": Will the Real "Consumer" Please Stand Up' (2016) 24 Competition & Consumer Law Journal 23, 23; Justin Malbon and Luke Nottage, *Consumer Law and Policy in Australia and New Zealand* (Federation

The definition of 'consumer' in this dissertation is significant, for two reasons. First, the major piece of legislation discussed in this dissertation, the ACL, contains a number of different definitions of consumer. 'Consumer' is defined both by itself and as part of the defined terms 'consumer goods' and 'consumer contracts'.[26] Second, two of the key sets of provisions contained in the ACL that are relevant to eObjects do not mention the word 'consumer' at all, namely:

1) section 18 of the ACL which prohibits misleading or deceptive conduct; and
2) sections 20–22 of the ACL which prohibit unconscionable conduct.

These provisions import an element of *commercial*, as opposed to purely *private*, activity, as the conduct prohibited must be in 'trade or commerce'. That is, private transactions will not be caught by these provisions. Examples of private transactions include one-off private sales of driverless cars, or connected homes, by individuals who are not carrying on a business.

Different definitions of 'consumer' have emerged due to a variety of factors. A recent survey of the different definitions used in Australia, New Zealand, the United Kingdom (**UK**), the European Union (**EU**) and the United States (**US**) indicated that most definitions depend on the existence of a good or service to be acquired.[27] The *variations* between these definitions reflect several factors, including:

Press 2013) 23–27; Geraint G Howells and Stephen Weatherill, *Consumer Protection Law* (Dartmouth 1995) 5.

[26] 'Consumer' is defined in ACL s 3. This definition applies in relation to consumer guarantees (ch 3 pt 3-2 div 1), unsolicited consumer agreements (ch 3 pt 3-2 div 3), lay-by sales agreements (ch 3 pt 3-2 div 3), itemised bills (ch 3 pt 3-2 div 4) and linked credit contracts (ch 5 pt 5-5 div 1). 'Consumer goods' is defined in ACL s 2 and applies to the product safety rules set out in ch 3 pt 3-3. 'Consumer contracts' is defined in s 23(3) and applies to the unfair contract terms provisions in ch 2 pt 2-3.

[27] O'Sullivan, 'The Definition of "Consumer": Will the Real "Consumer" Please Stand Up' (n 25) 28–41.

- who is doing the acquiring (for example, an individual, a small business, a listed company);
- the purpose for which the good or service is acquired (for a personal purpose or a business purpose); and
- the cost of the good or service.[28]

For simplicity, this dissertation defines a 'consumer' as an *individual* who has acquired, or is being persuaded to acquire, goods and/or services of a kind ordinarily acquired for personal, domestic or household use or consumption (adopting, in part, the ACL's definition in section 3). To limit its scope, this dissertation does not specifically consider purely private transactions (as discussed above). Nor does it consider the position of small businesses, although the argument is commonly (and often appropriately) made that these entities should be given the benefit of consumer protection regimes.[29] In general, the use of 'consumer' in this dissertation does not attempt to encompass wider concepts of individual 'users' of eObjects. These 'users' include many who are not consumers: that is, they have interactions with eObjects without entering into, or considering entering into, a contract for supply of an eObject or related service. They may not even be aware that they are having interactions with an eObject or associated system, and a term such as 'usee'[30] rather than 'user' may be more appropriate (see discussion in **section 3.3.2** of **Chapter 2**). The interests of users and usees who are not consumers are important for policymakers, but they are excluded from this dissertation purely for reasons of scope limitation. Some of the challenges for consumers *may* be challenges for other individual users and usees, as well as small businesses; but equally, there may be additional challenges for these other users and usees that fall outside the scope of this dissertation.

[28] Ibid.

[29] Ibid 41–44. For example, amendments to the unfair contract terms provisions in the ACL introduced protection for small businesses subject to unfair contract terms from 12 November 2016: see Treasury Legislation Amendment (Small Business and Unfair Contract Terms) Act 2015 (Cth).

[30] Eric Baumer 'Usees' (Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, April 18-23 2015).

3.5 The rise of the digital consumer

The concept of the 'consumer' cannot be fully considered without taking into account changes in the activities of consumers, marketers and suppliers that have taken place over the last 40 years. Such change can be roughly mapped into three phases: first, the 'traditional' activities engaged in through most of the twentieth century; second, the change in activities when what is now 'conventional' ecommerce became widely available;[31] and third, the change (still in progress) of activities relating to eObjects. 'Traditional' activities were engaged in well before the first 'wave' of computing discussed in **section 1.1** of this chapter. In contrast, the second and third phases of change were enabled by, and followed, the second and third 'waves' of computing.

Most of Australia's consumer protection laws were developed in response to the first phase, that is the 'traditional' forms of marketing, purchase and sale of goods and services developed in the twentieth century. These traditional forms saw suppliers marketing their goods and/or services to consumers either in person or mediated through print, radio and television, with consumers making most purchases in person, or via the post or telephone in response to printed catalogues. However, late in the twentieth century many suppliers and purchasers began moving past these traditional forms to new 'digital' technologies, that is:

> information and communication technologies (ICTs) that enable the production, storage and handling of information, and facilitate different forms of communication between human beings and electronic systems and among electronic systems in … binary computer language…[32]

New techniques in marketing and purchasing were developed to take advantage of the widespread availability of digital technologies such as

[31] For an examination of the history of ecommerce, see David F Rico, Hasan H Sayani and Ralph F Field, 'History of Computers, Electronic Commerce and Agile Methods' (December 2008) 73 Advances in Computers 1, 9–12.

[32] Eziyi O Ibem and Samuel Laryea, 'Survey of digital technologies in procurement of construction projects' (2014) 46 Automation in Construction 11, 12.

personal computing, the Internet, and the World Wide Web, creating the concept of the 'digital consumer'.

The second phase did not displace the first. Rather, it developed alongside it. 'Conventional' ecommerce is now commonplace, with many consumers regularly concluding contracts for purchase via digital means, such as a website or (less often) by email. These contracts are often made in response to consumers being exposed to advertising via a website or electronic message or after actively researching the product online. The rise of conventional ecommerce in the second phase has led to questions around the extent to which a 'digital consumer' or 'cyber consumer'[33] is distinct from an ordinary consumer, and whether this distinctiveness might give rise to legal problems.[34]

In conventional ecommerce, digital elements in the marketing and purchase process have had a significant effect on the way consumers are marketed to and the transactions undertaken.[35] Both advantages and disadvantages for consumers in conventional ecommerce have been identified. One advantage is an increased ability for consumers to compare terms and supplier reputation, while disadvantage may be found in the likelihood of a consumer being required to agree to far more detailed and onerous terms required for online compared to offline purchases.[36] Some commentators have argued that existing contract law is sufficiently adaptable to deal with any problems raised by electronic contracting, and therefore there is no need to create a

[33] Jerry Wind and Vijay Mahajan, 'Digital Marketing' (2002) 1 SYMPHONYA Emerging Issues in Management 43, 43.

[34] For example, John Rothchild, 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 Indiana Law Journal 893.

[35] Yoram Wind and Vijay Mahajan, 'Convergence Marketing' (2002) 16 Journal of Interactive Marketing 64.

[36] A comparison of advantages and disadvantages can be found in Kayleen Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (2011) 5 Studies in Ethics, Law, and Technology Article 4, 11-12; Robert Hillman and Jeffrey Rachlinski, 'Standard-Form Contracting in the Electronic Age' (2002) 77 *New York University Law Review* 429, 478-79.

sui generis regime.[37] However, other scholars have identified a range of legal problems arising out of activities enabled by conventional ecommerce. For example, legal problems have been identified specifically in the fields of: spam (unsolicited commercial electronic messages);[38] the formation of, and enforceability of onerous terms in, online contracts;[39] jurisdictional and choice of law issues in online contracting;[40] deceptive digital marketing practices;[41] and effects on consumer autonomy of persuasive techniques enabled by digital means.[42] However, legislative and judicial responses to these legal problems have, in general, been sparse and underdeveloped. An example of this is the somewhat casual acceptance of the enforceability of clickwrap online contracts by Australian judges.[43] Significant responses in Australia have been limited to the introduction of the Spam Act 2003 (Cth) (**Spam Act**), which regulates unsolicited commercial electronic messages,

[37] Juliet M Moringiello and William L Reynolds, 'From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting' (2013) 72 Maryland Law Review 452, 492; Leon E Trakman, 'The Boundaries of Contract Law in Cyberspace' (2008) 38 Public Contract Law Journal 187 ('wrap contracts are not sufficiently different from other forms of rolling contracts to warrant distinctive treatment': 190); Michael Furmston, GJ Tolhurst and Eliza Mik (contributor), *Contract Formation: Law and Practice* (2nd edn, OUP 2016) [6.02].

[38] Kayleen Manwaring, 'Canning the Spam Five Years On: A Comparison of Spam Regulation in Australia and the US' (2009) 76 Computers & Law 5.

[39] Nancy S Kim, *Wrap Contracts: Foundations and Ramifications* (OUP 2013); Margaret Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton UP 2013); Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (n 36); Edwin Wong and Adrian Lawrence, 'From Shrink to Click and Browse: Ensuring the Enforceability of Web Terms' (2004) 7 Internet Law Bulletin 61.

[40] Nick James, 'Online Contracts, Electronic Signatures and the Law' (2000) 36 Australian Property Journal 283.

[41] Rothchild, 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (n 34); Victor T Nilsson, 'You're Not from Around Here, Are You? Fighting Deceptive Marketing in the Twenty-First Century' (2012) 54 Arizona Law Review 801.

[42] Ryan Calo, 'Digital Market Manipulation' (2014) 82 George Washington Law Review 995; Eliza Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 Law, Innovation and Technology 1; Natali Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Publishing 2016).

[43] Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (n 36) 6–10.

and the passing of electronic signatures legislation.[44] Other jurisdictions have seen more substantial developments, such as the EU's directives and proposals relating to online sales and sales of digital content.[45] However, not all of these developments have been successful or widely accepted. The attempt at a model law in the US in the form of the Uniform Computer and Information Transactions Act (**UCITA**)[46] faced fierce opposition, and eventually was only adopted in two US states.[47]

The introduction of *mobile* ecommerce, using smartphones and similar devices, heralded the transition to the third phase. With the advent of eObjects, the concept of a 'digital consumer' is no longer confined to an individual sitting in a darkened room in front of a computer screen. Consumer activities are now more likely to occur in the physical world *outside* the dark room, as the variety and nature of the digital technologies used for marketing and purchasing change. In particular, digital marketing can now be aimed at a consumer almost anywhere and at any time. However, 'third phase' digital consumers are not characterised solely by this shift in the location of marketing activities. They also tend to face increasing complexity in the information that is provided to them, or which they require, in order to understand products and services. Also, this information is provided via

[44] Electronic Transactions Act 1999 (Cth) and its state equivalents (although note there are slight variances between the different pieces of legislation): Electronic Transactions Act 2001 (ACT); Electronic Transactions Act 2000 (NSW); Electronic Transactions Act 2000 (NT); Electronic Transactions Act 2001 (Qld); Electronic Transactions Act 2000 (SA); Electronic Transactions Act 2000 (Tas); Electronic Transactions Act 2000 (Vic); Electronic Transactions Act 2003 (WA).

[45] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1; Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L304/64; Amended Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods COM(2017) 637.

[46] Available at 'Computer Information Transactions Act' (15 October 2002) <https://my.uniformlaws.org/viewdocument/final-act-with-comments-14?CommunityKey=92b2978d-585f-4ab6-b8a1-53860fbb43b5&tab=librarydocuments> accessed 22 December 2018.

[47] UCITA was drafted by the National Conference of Commissioners on Uniform State Laws; however, it has not been eagerly embraced by the state governments for which it was intended: Nim Razook, 'The Politics and Promise of UCITA (Uniform Computer Information Transactions Act)' (2003) 36 Creighton Law Review 643.

an increasing variety of devices. These devices may have more than one function, and the information delivered to consumers through these devices may not be easily identified as containing marketing messages. Many 'traditional' brick-and-mortar forms of purchase may now include some form of digital mediation, and new forms of both marketing and purchasing are emerging.

Chapter 4 develops a series of vignettes (the '**Vignettes**') to provide real-life examples of this third phase. For example, some consumers are currently being tracked by marketers while 'out and about' in physical space rather than cyberspace and are receiving personalised marketing communications relevant to their specific geographic locations on their personal connected devices, such as smart watches. Even when consumers are at home, they do not have to make the conscious decision to sit down at their computer to purchase. They can be involved in another activity, such as making coffee, and make a purchase in one click, or with one voice command, without leaving the kitchen.

4 SIGNIFICANCE AND CONTRIBUTION

4.1 Significance of the research

> It is well known that mobile commerce and pervasive computing create new commercial opportunities. At the same time, they raise problems in relation to the legal framework that surrounds them.[48]

This research is intended to make a contribution to the contemporary and developing issue of the nature of the legal implications of sociotechnical change brought about by eObjects. It aims to assist in filling a literature gap by analysing the likely application of relevant areas of consumer protection law in Australia to this change. In particular, it aims to provide assistance to

[48] Pernille Wegener Jessen and Rene Franz Henschel, 'Editorial: Special Issue on Legal Aspects of Mobile Commerce and Pervasive Computing: Privacy, Marketing, Contracting and Liability Issues' (2011) 4 International Journal of Private Law 185, 185.

policymakers, legislators, regulators and judges in analysing existing law and coming to conclusions about its meaning and adequacy.

Existing and emerging markets in eObjects in the industrial, agricultural, health, vehicle, utilities and home automation areas are already significant globally. In August 2018, one analytics firm estimated the number of connected devices globally to be 7 billion, and the global 'IoT' market value to be USD151 billion.[49] Predictions as to growth in the market for eObjects vary considerably,[50] but some estimates of market value extend into the trillions of US dollars, with actual connected devices well into the billions, by 2020.[51] However, at least some of the largest growth projections[52] are likely affected by the global culture of 'hype' surrounding emerging technologies and markets.[53] A specific example of growth in a subsection of the industry can give firmer shape to these estimates. According to the technology research firm Telsyte, in 2017 the Australian market for eObjects in the home

[49] Knud Lasse Lueth, 'State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating' (*IoT Analytics,* 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> accessed 14 February 2019. These numbers *exclude* 'smartphones, tablets, laptops or fixed line phones'.

[50] See for example, Louis Colombus, 'Roundup of Internet of Things Forecasts and Market Estimates: 2018' (*Enterprise Irregulars,* 2 January 2018) <www.enterpriseirregulars.com/121867/roundup-internet-things-forecasts-market-estimates-2018/> accessed 27 August 2018, which lists a series of different reports and predictions on market growth for the Internet of Things.

[51] Ibid. Gartner's estimate in September 2018 was 20 billion connected devices by 2020: Bob Gill and David Smith, *The Edge Completes the Cloud: A Gartner Trend Insight Report* (14 September 2018).

[52] Gartner's very large estimate (set out in n 51) is still considerably lower than the figure of 50 billion which is more popularly, but questionably, quoted: Amy Nordrum, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated' (*IEEE Spectrum*, 18 August 2016) <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated> accessed 26 September 2018.

[53] Gil Press, 'It's Official: The Internet of Things Takes Over Big Data As the Most Hyped Technology' (*Forbes*, 18 August 2014) <www.forbes.com/sites/gilpress/2014/08/18/its-official-the-internet-of-things-takes-over-big-data-as-the-most-hyped-technology/#10c29f111aaa> accessed 27 August 2018.

grew 55% to AUD583 million, and in 2018, there was an average of 17.1 Internet-connected devices in each household, up from 11.1 in 2016.[54]

Despite the importance of the area to industry and to consumers, in the first two years of research for this doctorate (the author enrolled part-time in 2013), the original literature survey indicated that scholarly, and indeed practitioner, consideration of the effects of eObjects on commercial activities in Australian and international markets was very limited.[55] This situation changed dramatically over the course of candidature, as outlined in **section 4.1.3** of this chapter, particularly in relation to commentary by European and North American scholars. Australian scholarship, while developing,[56] remains limited, as set out in **sections 4.1.1**, **4.1.2** and **4.1.3** of this chapter.

4.1.1 The early scholarly literature

The conversation in the legal literature began with an article in 2005 by Kang and Cuff (law and architecture professors, respectively) who outlined a ground-breaking vision of a mixed real/virtual shopping centre using existing and future eObject technologies. In such a shopping centre (translating Kang and Cuff's examples to an Australian context), a customer might enter the

[54] Telsyte, 'Smart Speakers Help Send Australian IoT@Home Market Skyward' (*Announcements,* 15 May 2018) <www.telsyte.com.au/announcements/2018/5/15/smart-speakers-help-send-australian-iothome-market-skyward> accessed 19 June 2018. The Telsyte research included two online surveys of representative samples of Australians aged 16 years and over, each with over 1000 respondents.

[55] For example, Jessen and Henschel, 'Editorial: Special Issue on Legal Aspects of Mobile Commerce and Pervasive Computing: Privacy, Marketing, Contracting and Liability Issues' (n 48); Grace Li, 'Deciphering Pervasive Computing: A Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' in Varuna Godara (ed), *Risk Assessment and Management in Pervasive Computing: Operational, Legal, Ethical and Financial Perspectives* (Information Science Reference 2009); Grace Li, 'What We Know and Do Not Know: The Legal Challenges for International Commercial Contract Formation in a Pervasive Computing Environment' (2011) 4 International Journal of Private Law 252.

[56] See for example, Megan Richardson and others, 'Privacy and the Internet of Things' (2016) 21 Media & Arts Law Review 336; Megan Richardson and others, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' (2017) 6 Internet Policy Review; Kate Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (SJD minor thesis, Bond University 2017).

centre, go into a department store, look at the child restraints on display, take out her smartphone to look at product review and price comparison sites and then buy a restraint from a completely different store with a mobile shopping application. Her smartphone could then alert her to a shopping task she has forgotten. Consequently, she might check the shopping list created by her smart refrigerator and be diverted to the supermarket to buy milk and bread. Her incidental movement through the shopping centre may lead to the collection of information about which store windows she looks into, her use of e-loyalty cards, and her consumption of pink-iced doughnuts.

Kang and Cuff were interested in examining the effect of the use of 'pervasive computing' (a subset of eObjects) on the laws affecting the public sphere. They concluded that this vision of a shopping centre with embedded and mobile information technologies produced a significant need for legal development in areas as diverse as contract law, property law, privacy and telecommunications regulation. Moving out of the commercial sphere, the next year Brenner undertook a significant analysis of pervasive technology in the context of the criminal law.[57]

Soon afterwards, concerns about the exponentially greater data collection capacity of these technologies began to be raised. In 2007, Werbach published a study of sensor-based technologies. He concluded that many legal rules, such as those contained in evidence law, corporate disclosure regulation, civil and criminal procedure, and patents law, were likely to become problematic as they were based on an information scarcity model that would be superseded by the predicted growth in data collection enabled by such technologies.[58] A few years later Walker Smith articulated similar concerns about the effect of the increasing amount of information available, but in the context of sellers' capacity to know progressively more about the

[57] Susan W Brenner, 'Law in an Era of Pervasive Technology' (2006) 15 Widener Law Journal 667; Susan W Brenner, *Law in an Era of 'Smart' Technology* (OUP 2007).
[58] Kevin Werbach, 'Sensors and Sensibilities' (2007) 28 Cardozo Law Review 2321.

way consumers use their products. He predicted an increase in product liability claims based on a greater ability of suppliers to foresee harms.[59]

In 2009 and 2011, the Australian scholar Li sketched preliminary concerns regarding privacy, security, jurisdictional and international contract formation issues arising from pervasive computing.[60] Despite the fact that the privacy and security issues are the themes that have received most attention in the literature to date, these concerns remain largely unresolved at the time of writing of this dissertation. Moving on from the privacy and security issues, in 2012 Fairfield undertook a preliminary examination of the divergence of 'online and offline law',[61] and considered the difficulties this might cause when virtual experiences are mixed with real-life experiences. He examined technologies such as mobile phone applications which display images and videos when they are pointed at real objects, such as museum exhibits. Fairfield raised a concern that the US courts, when faced with lawsuits involving augmented reality applications, may apply intellectual property laws (particularly copyright) that might limit the re-use of purchased items, rather than consider 'real-world' implications under contract law and property law. Interestingly, Kang and Cuff had identified the opposite problem. They were concerned that their hypothetical shopping centre owners would assert their private property rights over Internet connectivity ports within the shopping centre to shape and control information flowing to their customers.

In Peppet's work, published in the same year as Fairfield's, the effect on consumers also emerged as an important theme. Peppet concentrated on the impact of eObjects with augmented reality applications on the law of

[59] Bryant Walker Smith, 'Proximity-Driven Liability' (2013–14) 102 Georgetown Law Journal 1777.

[60] Li, 'Deciphering Pervasive Computing: A Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' (n 55); Li, 'What We Know and Do Not Know: The Legal Challenges for International Commercial Contract Formation in a Pervasive Computing Environment' (n 55).

[61] Joshua Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (2012) 27 Berkeley Technology Law Journal 55, 55.

consumer contracts. He provided a preliminary analysis of some of the possible effects of eObjects on contract law and the impact of underlying technological conditions on doctrine. In particular, he argued that because consumers have greater access to information about products and about onerous contract terms, US courts should be less likely to hold a contract unenforceable on the ground of unconscionability or related 'unfairness' grounds.[62]

Unsurprisingly, in all of these early responses, the authors provided only preliminary analyses of both the issues and the relevant legal problems. The enquiry in this dissertation is both broader and deeper than the works discussed above in that it: tends to cover a wider range of technologies; a wider range of consumer challenges; and a more in-depth doctrinal analysis of existing law and its application to sociotechnical change.

4.1.2 Other responses

In addition to scholarly work, significant concerns have been expressed by consumer and other interest groups worldwide about the possible disbenefits of eObjects.[63] Even industry groups set to capitalise on the growing market are expressing concerns, particularly in the area of cybersecurity.[64] For example, in 2017, Australia's peak industry body associated with eObjects,

[62] Scott R Peppet, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (2012) 59 UCLA Law Review 676, 736–45.

[63] Liz Coll and Robin Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (Consumers International, April 2016), updated in Consumers International, *Testing Our Trust: Consumers and the Internet of Things 2017 Review* (October 2017); Alexander Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (Australian Communications Consumer Action Network, February 2016); ANEC and others, *Securing Consumer Trust in the Internet of Things: Principles and Recommendations 2017* (November 2017); Karen Rose, Scott Eldridge and Lyman Chapin, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (Internet Society, October 2015).

[64] Geof Heydon and Frank Zeichner, *Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act* (Industry Report, Communications Alliance, October 2015).

IoT Alliance Australia, issued a guide for business[65] and two successive versions of an Internet of Things Security Guideline[66] in an attempt to deal with emerging concerns about the security of eObjects. Overseas government departments and international policy bodies have also begun to look past the promise of the new technology, and respond to concerns about its regulatory implications.[67]

On 28 September 2018, the Governor of California approved a law requiring manufacturers to equip 'connected devices' with reasonable security features, commencing on 1 January 2020.[68] On 11 March 2019, a bipartisan Bill, the proposed Internet of Things Cybersecurity Improvement Act of 2019, was introduced into the US Senate.[69]

Despite these developments, until recently Australian legislators and policymakers were slow to identify and respond to the challenges raised by eObjects, preferring instead to concentrate on the positive aspects. An initial interest in issues surrounding 'mobile technologies' shown by the Australian

[65] IoT Alliance Australia, *Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia: V1.0* (November 2017).

[66] IoT Alliance Australia, *Internet of Things: Security Guideline: V1.0* (February 2017); IoT Alliance Australia, *Internet of Things Security Guideline: V1.2* (November 2017).

[67] United States, Department of Commerce, National Telecommunications and Information Administration, *Green Paper: Fostering the Advancement of the Internet of Things* (January 2017); Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (January 2015); United Kingdom, Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the Cyber Security of Consumer Internet of Things* (Report, 7 March 2018); European Union, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things (16 September 2014); European Commission, *Report of Internet of Things Privacy and Security Workshop*; OECD, *Consumer Policy and the Smart Home* (OECD Digital Economy Papers No 268, April 2018); OECD, *Consumer Product Safety in the Internet of Things* (OECD Digital Economy Papers No 267, March 2018).

[68] Security of Connected Devices, Cal Civ Code §§ 1798.91.04–06.

[69] S. 184, 116th Congress (2019). This Bill is a successor of two failed Bills from 2017 and 2018. Katharine Goodloe and Micha Nandaraj Gallo, 'Senate Reintroduces IoT Cybersecurity Improvement Act' (*Global Policy Watch,* 13 March 2019) <www.globalpolicywatch.com/2019/03/senate-reintroduces-iot-cybersecurity-improvement-act/> accessed 7 April 2019.

Law Reform Commission in 2013 was not pursued.[70] In 2015, the Hon Malcolm Turnbull (then Communications Minister) urged 'minimal' regulation of this area of sociotechnical change.[71] Later the same year, the Australian Communications and Media Authority (**ACMA**) released an occasional paper[72] concentrating on spectrum and numbering issues. Concerns around privacy, reliability, operability and complexity of connections were mentioned very briefly. However, the paper concluded that 'the balance of regulatory interventions in the future is likely to skew more towards … enabling strategies … to encourage innovation and the adoption of IoT applications'.[73] The consultation process invited little public attention.[74] There have also been some indications of active reluctance to deal with this issue. In 2016–17, Consumer Affairs Australia and New Zealand (**CAANZ**) conducted a review of the ACL. The interim report mentioned some concerns raised by submissions about the applicability of the ACL (particularly consumer guarantees) to the 'internet of things'.[75] However,

[70] Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, May 2013) particularly pt 5.

[71] Angus Kidman, 'Malcolm Turnbull: The Internet of Things Relies on Imagination, not Regulation' Lifehacker (26 March 2015) <www.lifehacker.com.au/2015/03/malcolm-turnbull-the-internet-of-things-relies-on-imagination-not-regulation/> accessed 20 June 2016.

[72] Australian Communications and Media Authority, *The Internet of Things and the ACMA's Areas of Focus: Emerging Issues in Media and Communications* (Occasional Paper, November 2015) <www.acma.gov.au/theACMA/~/media/18E314A0C00A41F9B4D629DAB9397436.ashx> accessed 20 June 2018.

[73] Ibid 30.

[74] ACMA received only three submissions to its public inquiry on the occasional paper. Only two were published, one from NBN and one from Telstra. See Australian Communication and Media Authority, *The Internet of Things and the ACMA's Areas of Focus: Emerging Issues in Media and Communications* (Occasional Paper, November 2015) <www.acma.gov.au/theACMA/~/media/18E314A0C00A41F9B4D629DAB9397436.ashx> accessed 30 June 2018.

[75] Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review: Interim Report* (October 2016) 203. Note this report uses lower case for the term 'internet of things'.

CAANZ's *final* report made no specific mention of these issues, relegating the examination of 'emerging technologies' to 'issues for future exploration'.[76]

However, since the commencement of this doctoral study there has emerged a growing policy focus on problems relating to the collection, use and dissemination of data by public and private actors. This has led to some limited but increasing interest in eObjects by government and policy organisations. Progress on the regulatory front has been minimal and the problems have not been deeply explored. However, Australian governments and agencies are now beginning to show some concern about disbenefits. For example, the Productivity Commission's 2017 report on data use and availability mentioned the increasing use of eObjects as sources of data collection,[77] and contained a case study which included some examples of eObjects and potential disbenefits.[78] On 21 May 2018, the Australian Government announced an AUD208,595 grant to the Australian Council of Learned Academies (**ACOLA**) to 'examine the opportunities, risks and consequences of the IoT, and consider ways to foster technological leadership while ensuring responsible deployment'.[79] In July 2018, the Human Rights Commission (**HRC**) released an issues paper as part of its Human Rights and Technology Project, which mentioned briefly that

[76] Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review: Final Report* (March 2017) 28.

[77] Productivity Commission, *Data Availability and Use* (Productivity Commission Inquiry Report No 82, March 2017) 71, 569–94.

[78] Ibid 569–94.

[79] Ministers for the Department of Industry Innovation and Science Senator Matt Canavan and Karen Andrews MP and Minister for Education Senator Simon Birmingham, 'Funding to Advance New Scientific and Technological Developments' (Media Release, 21 May 2018) <www.minister.industry.gov.au/ministers/cash/media-releases/funding-advance-new-scientific-and-technological-developments> accessed 14 November 2018. The project, called 'The Internet of Things: Maximising the benefit of deployment in Australia' was awarded through the Australian Research Council's Linkage Learned Academies Special Projects program Supporting Responses to Commonwealth Science Council Priorities. See Australian Council of Learned Academies (ACOLA), 'ACOLA Receives ARC Funding to Undertake Two New Horizon Scanning Projects on AI and IoT' (Media Release, 21 May 2018) <https://acola.org/artificial-intelligence-internet-of-things/> accessed 12 September 2019.

eObjects could 'present … platforms for cybercrime'.[80] In August 2018, the author of this dissertation participated in a joint submission to the HRC based on the research undertaken during doctoral study, on the basis that the challenges raised by eObjects extended well beyond cybercrime. Such sociotechnical change can 'also have negative implications for human rights to privacy, safety and security, non-discrimination and equal treatment.'[81] The Australian Competition and Consumer Commission (**ACCC**) recognised a number of challenges posed by eObjects as part of the recent Digital Platforms Inquiry, but found that the 'wider impact'[82] of such technologies was still too unclear to form a foundation for specific recommendations to government other than that policymakers should 'actively engage with the implications of these developments when formulating policy, and considering regulatory reform'. [83]

4.1.3 How this dissertation fits within the literature

Issues relating to the use and misuse of data are important, and are rightly fuelling increasing concerns from consumers, policymakers and legislators. However, an exclusive focus on data issues runs the risk of ignoring one of the key common features of eObjects: their existence as part of a cyber-*physical* system. As discussed in **Chapter 2** of this dissertation, the active capacity of many eObjects means that they can act on the physical world around them, and their impact is not confined to data collection, processing and dissemination.

Considering all of the concerns discussed in **sections 4.1.1** and **4.1.2** of this chapter, the likelihood of legal problems arising out of sociotechnical change as a result of the third wave is high. The realisation of this likelihood is what

[80] Human Rights Commission, *Human Rights and Technology* (Issues Paper, July 2018) 16.

[81] A Yu and others, *Response to Issues Paper on Human Rights and Technology* (2018) 2.

[82] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (June 2019) 503. See also Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (December 2018) 301.

[83] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (n 82) 518.

motivated the first draft of this dissertation research proposal in 2012, and the emerging discussion since that time has only underscored its importance.

By late 2015, research for this dissertation had identified two significant gaps in the technical, legal and policy literature. First, a search for a useful definition of third wave technologies was problematic. Many different terms had been used, but their uses and definitions were inconsistent and conflicting, dependent on geographical locations, individual researchers, and change over time. To overcome these problems, a historical and analytic review of the technical literature was undertaken, abstracting the attributes of and interactions among the technologies at issue. In 2015, the author of this dissertation published an article[84] outlining these attributes and interactions as part of a technical research framework on which a legal, business or policy analysis could be based. The technical research framework developed in this article, updated to include new examples of eObjects, now forms **Chapter 2** of this dissertation. This article was submitted to the US Department of Commerce (**USDC**) as part of a submission to the US Federal Government's inquiry into 'The Benefits, Challenges and Potential Roles for the Government in Fostering the Advancement of the Internet of Things'. The contention in this article that the term 'Internet of Things' was a 'misnomer' was accepted by the USDC in a green paper published as part of the inquiry.[85] Despite this acknowledgement, the USDC continues to use the term 'for the sake of simplicity'.[86] The utility of an attributes-based approach was also illustrated by UK researchers in 2016 and 2017 who built a list of

[84] Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (2015) 31 Computer Law & Security Review 586.

[85] United States, Department of Commerce, National Telecommunications and Information Administration, *Green Paper: Fostering the Advancement of the Internet of Things* (n 67) 7.

[86] Ibid 7.

attributes to assist in identifying legal problems in the context of eObjects and cloud computing.[87]

The second major gap was identified in the legal literature. Until late 2015, most of the discussion of eObjects had concentrated on the inadequacy of existing data protection and privacy laws, and, to a more limited extent, security.[88] These are undeniably important to consumers, and will only increase in importance. However, they do not tell the whole story. Only a small amount of earlier literature, other than that mentioned above, raised misgivings about other effects on consumers and their contracts with suppliers, and even in these articles the discussion of eObjects was brief and preliminary.[89]

In January 2016, in an attempt to address that gap, the author of this dissertation completed and distributed on SSRN.com a research paper,[90] later published in revised form as a journal article.[91] This paper detailed the

[87] W Kuan Hon, Christopher Millard and Jatinder Singh, 'Twenty Legal Considerations for Clouds of Things' (Queen Mary School of Law Legal Studies Research Paper No 216, 2016) <http://ssrn.com/abstract=2716966> accessed 14 July 2018. An abbreviated version of this working paper was later published as Christopher Millard, W Kuan Hon and Jatinder Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (Proceedings of the 2017 IEEE International Conference on Cloud Engineering, Vancouver, 4-7 April 2017).

[88] For example, Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85; Adam Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation' (2015) 21 Richmond Journal of Law & Technology 6; James Ridge, 'What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive' (2007–08) 49 South Texas Law Review 725.

[89] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88); Nancy S Kim, 'Two Alternate Visions of Contract Law in 2025' (2014) 52 Duquesne Law Review 303; Jerry Kang and Dana Cuff, 'Pervasive Computing: Embedding the Public Sphere' (2005) 62 Washington and Lee Law Review 93; Miriam A Cherry, 'A Eulogy for the EULA' (2014) 52 Duquesne Law Review 335; Calo, 'Digital Market Manipulation' (n 42).

[90] Kayleen Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (UNSW Law Research Paper No 2016–15, 2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690024> accessed 18 May 2018.

[91] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

conceptual framework outlined in **Chapter 3** of this dissertation and showed how the conceptual framework adopted could be used to uncover legal problems arising out of eObjects. It provided examples in the areas of product liability, anti-hacking legislation, consumer protection, contract, and intellectual property. At around the same time, evidence of greater concern about challenges for consumers acquiring and interacting with eObjects that fell outside the data protection and security issues began emerging in the publications of some government departments and consumer groups.[92] Later in 2016, and years following, a body of overseas academic literature began emerging regarding concerns arising not only in relation to the attributes of eObjects themselves,[93] but also out of contractual arrangements used to supply them to consumers and the way that contractual terms were delivered.[94]

The technical research framework in **Chapter 2** of this dissertation, coupled with a review of the academic and policy literature, formed the basis for the broad identification of the main eObject-related challenges for consumers whose outcomes had the potential to conflict with consumer protection goals. The results of this research were published online as a journal article in August 2017,[95] and this article forms the basis for **Chapter 5** of this

[92] For example, Rose, Eldridge and Chapin, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (n 63); Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63); Vulkanovski, *'Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63).

[93] See for example, Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42); Christiane Wendehorst, 'Consumer Contracts and the Internet of Things' in Reiner Schulze and Dirk Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Publishing 2016).

[94] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93); Guido Noto La Diega and Ian Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7 European Journal of Law and Technology; Stacy-Ann Elvy, 'Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond' (2016) 44 Hofstra Law Review 839.

[95] Kayleen Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (2017) 17 Oxford University Commonwealth Law Journal 265.

dissertation. The importance of identifying these challenges and their conflicts with key consumer principles for developing public policy internationally was highlighted by the multiple citations of this article in an Organisation for Economic Co-operation and Development (**OECD**) report[96] published in April 2018. This report was prepared as part of the OECD's Going Digital project,[97] which is aimed at 'help[ing] policymakers better understand the digital transformation that is taking place and create a policy environment that enables their economies and societies to prosper in a world that is increasingly digital and data-driven'.[98] A statement justifying this project tellingly recognises that 'the digital economy offers challenges as well as opportunities'.[99]

Subsequent to the publication of the August 2017 article by the author of this dissertation on consumer challenges, some of the same challenges were emphasised in Mathews-Hunt's minor dissertation.[100] Mathews-Hunt's dissertation drew significantly on some of the previously published work of the author of this dissertation,[101] some of which is now integrated into this dissertation. Mathews-Hunt's work remains (as of 30 June 2018) the only Australian scholarly work (other than this dissertation and the author's

[96] OECD, *Consumer Policy and the Smart Home* (n 67) 23.

[97] OECD, 'Going Digital: Making the Transformation Work for Growth and Well-Being' (*OECD*) <www.oecd.org/going-digital/project/> accessed 31 July 2018.

[98] OECD, *Going Digital in a Multilateral World: An Interim Report to Ministers* (Meeting of the OECD Council at Ministerial Level, Paris, 30–31 May 2018) 9.

[99] Douglas Frantz, 'Going Digital: Making the Transformation Work for Growth and Well-Being' (*OECD*, 24 January 2017) <www.oecd-forum.org/channels/722-digitalisation/posts/17393-going-digital-making-the-transformation-work-for-growth-and-well-being> accessed 11 June 2018.

[100] Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56).

[101] In particular, Manwaring and Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (n 84); Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (n 90). Also (bibliography only) Kayleen Manwaring, 'Data Breach Notifications: An Australian Perspective' (2009) Privacy and Data Security Law Journal 848; Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (n 36); Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2); Manwaring, 'Surfing the Third Wave of Computing: Contracting with eObjects' (n 3).

previously published papers in 2015–18 which are reproduced in part in it) that considers consumer protection law in any significant detail in relation to eObjects,[102] although there are some brief mentions elsewhere, particularly in short practitioner articles.[103]

The analysis set out in **Chapter 5** revealed many challenges for consumers arising out of eObjects that may give rise to legal problems. One of the most important of these provided the foundation for the in-depth legal analysis set out in **Chapter 6.** This challenge consisted of the possibility of manipulation of consumer behaviour by commercial entities, facilitated by both the data collection capacities of eObjects and their current and potential uses as marketing channels. Public concern about the use of data for manipulation of the general public came to the fore in the wake of the Cambridge Analytica scandal, where Facebook data was allegedly used by commercial and state actors to manipulate voters and influence the outcomes of elections.[104] By 2014 the US scholar Calo had already provided a substantial examination of the possibility of data collected online being used for manipulation of consumers by commercial entities for the purposes of increasing sales.[105] This was a theme later elaborated upon by other scholars

[102] In contrast, there is some Australian literature that considers the *privacy* implications in detail. For example, Richardson and others, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' (n 56); Richardson and others, 'Privacy and the Internet of Things' (n 56); Rachelle Bosua and others, 'Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective' (2017) Networked Society Institute Research Paper 6; Xavier Caron and others, 'The Internet of Things (IoT) and Its Impact on Individual Privacy: An Australian Perspective' (2016) 32 Computer Law & Security Review 4.

[103] James Halliday and Rebekah Lam, 'Internet of Things: Just Hype or the Next Big Thing?' (2015) 34 Communications Law Bulletin 7; James Halliday and Rebekah Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (2016) 34 Communications Law Bulletin 4.

[104] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (Sydney, 18 March 2018) <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 18 March 2018.

[105] Calo, 'Digital Market Manipulation' (n 42). See also Ryan Calo, 'Tiny Salespeople: Mediated Transactions and the Internet of Things' (2013) 11 IEEE Security & Privacy Magazine 70. However, note that Calo was not the first to be concerned about manipulation based on digital information. See for example, Arthur Raphael Miller, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Michigan UP 1971) 42–

in relation to UK and European law.[106] Extending this theme, a major objective of the in-depth analysis undertaken for this dissertation has been to assess whether eObjects and the systems in which they participate would provide opportunities for more effective manipulation of consumers, and if so, whether or not current Australian law would be sufficient to protect consumers from resulting harms.

In a 2016 research paper[107] and subsequent 2017 article,[108] both by the author of this dissertation, this issue was raised in a preliminary form. In November 2017 and April 2018, the author of this dissertation also presented conference papers at two conferences (one in Australia and one in the UK) delineating the detailed doctrinal analysis of the current Australian consumer protection laws.[109] This doctrinal analysis was also published as a journal article in December 2018.[110] A discussion of the research on this issue now constitutes **Chapter 6** of the dissertation.

In summary, this dissertation assists in filling a significant gap in the scholarship surrounding areas of emerging technologies that are set to have an increasing impact on both consumers and commercial entities.

43; PM Schwartz and DJ Solove, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814, 1850.

[106] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42); Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42).

[107] Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (n 90).

[108] Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

[109] Kayleen Manwaring, 'Digital Consumer Manipulation Enabled by Emerging Technologies' (British and Irish Law Education and Technology Association Conference, Aberdeen, April 2018); Kayleen Manwaring, 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (Law, Technology & Innovation Junior Scholars Forum, UNSW Kensington, 24 November 2017).

[110] Kayleen Manwaring, 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (2018) 26 Competition and Consumer Law Journal 141.

4.2 Original contribution

This dissertation contributes significant original research in the discipline of law and technology in several areas.

First, in **Chapter 2** this dissertation attempts to resolve long-standing problems of definition. It has extracted from myriad different descriptions of the technology a framework of attributes and interactions for the technologies in issue. This technical research framework provides a basis for a range of legal, business strategy and policy research relating to this particular technological area. This framework of attributes and interactions is also used in **Chapter 4** as a basis for a series of hypothetical Vignettes developed to illustrate the new things, activities and relationships enabled by eObjects.

Second, in **Chapter 5** this dissertation identifies the major challenges for consumers arising out of the development, sale and use of eObjects whose outcomes conflict with the goals of Australia's consumer protection laws. These challenges were systematically identified by analysis of the attributes and interactions developed in the technical research framework, supplemented by examination and consolidation of a wide range of research from consumer groups, industry and scholars, and illustrated by creation of hypothetical vignettes.

Third, in **Chapter 6** this dissertation identifies and examines in detail the legal problems arising in Australia relating to the protection of consumers against digital consumer manipulation under the ACL. It does this by applying the conceptual framework and research approach set out in **Chapter 3**. As a result, a further contribution is made to evaluating the effectiveness of this conceptual framework and approach in applying it to a particular type of sociotechnical change.

Fourth, in **Chapter 7**, first steps are taken in establishing what can be done to 'reconnect' consumer protection law with the consumer harms brought about by digital consumer manipulation enabled by eObjects. This chapter proposes in broad terms the basic principles and some of the major features

that should be adopted in legal frameworks that attempt to move the existing law closer to achieving the goals underlying consumer protection law in Australia.

5 RESEARCH APPROACH

5.1 The nature of doctrinal research

A doctrinal methodology was chosen for the research underlying this dissertation. Doctrinal research has been described as 'the systematic exposition, analysis and critical evaluation of legal rules and their relationships'.[111] While doctrinal research traditionally examines the systematisation and classification of existing law, Roux argues that good doctrinal research should also aspire to 'push … through settled legal questions to address questions that are complex and unresolved in the legal system'.[112] This methodology is well suited to examining problems around the law and emerging technologies, especially as:

> new technological developments may throw up novel questions of liability for harm caused. In this instance, good doctrinal research will anticipate the types of question that might arise in litigation and suggest how they ought to be decided. It may also suggest the need for law reform to the extent that the problems arising are not amenable to judicial resolution.[113]

As discussed in **Chapter 3**, an assumption that new technological developments will *always* give rise to novel questions of law is not able to be supported. The critical term in the quote above is 'may'. The critical evaluation of legal rules required by a doctrinal methodological approach

[111] Council of Australian Law Deans, *CALD Statement on the Nature of Legal Research* (May and October 2005) 1, paraphrasing the definition in Dennis Pearce, Enid Campbell and Don Harding, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (1987) paras 9.10–9.15.

[112] Theunis Roux, 'Judging the Quality of Legal Research: A qualified Response to the Demand for Greater Methodological Rigour' (2014) 24 Legal Education Review 173, 183.

[113] Ibid.

can reveal that existing legal classifications and rules apply quite uncontroversially, despite particular kinds of sociotechnical change brought about by new technologies. Or it can reveal the opposite, that new things, activities and relationships arising out of the sociotechnical change are indeed of such a type that they do not fit well within existing rules.

In examining the sociotechnical change brought about by eObjects, the research questions posed in this dissertation require an understanding of 'how [the law] ought to be understood and how it might be improved',[114] in circumstances where it impacts upon consumer transactions involving eObjects. The ultimate aim of this research is common to most doctrinal research: that is, 'clearly and succinctly to express the norms (principles, standards and rules) that have been established [and then] creatively to develop the implications of settled law for unresolved questions'.[115]

However, academic, legislative and judicial discussion of the law in this area in Australia has been quite sparse. Even though the volume of academic commentary concerning eObjects is increasing every year, there are few specific primary law sources. To confine this dissertation to examining only the Australian doctrinal landscape runs the risk of missing important issues, as will be the case for many doctrinal research projects relating to emerging technologies and sociotechnical change. Therefore, this dissertation also undertakes some comparison with law from other jurisdictions. The limitations of the comparative methodology employed are also discussed in the following section.

5.2 A narrowly focussed comparative approach

In order to make a rigorous assessment of legal problems concerning consumer transactions relating to eObjects, this dissertation also examines law and commentary relating to eObjects in jurisdictions outside of Australia. In particular, law and commentary in the US and EU will be

[114] Ibid 175.
[115] Ibid 183.

examined, the latter at the level of pan-European law, not individual European countries. These jurisdictions were chosen due to their high levels of investment in the relevant technologies, and the level of interest shown by their regulators and commentators.

Clark defined comparative legal research as 'the science or practice of identifying, explaining, or using the similarities and differences between two or more legal systems or their constituent parts'.[116] Unlike some forms of comparative law research, the examination of foreign law and commentary in this dissertation is narrowly focussed. It concentrates on the last component of Clark's description. Comparative legal research in a narrow form has recently been recognised as a subset or type of doctrinal research.[117] This reflects the fact that it has become a common (if generally unacknowledged) feature of doctrinal research in the last 40 years.[118] In the context of doctrinal research, the comparison can be undertaken in different forms, the amount of comparison required falling along a spectrum.[119] The comparison can range from a 'microcomparison'[120] of rules used to solve specific problems, to a comparison on a larger scale of the 'general patterns and themes' of the different systems.[121]

The comparative approach in this dissertation is confined to the narrow end of the scale, examining specific examples of legal rules and commentary of relevance. It has been employed in this dissertation solely as a useful

[116] David S Clark, 'Comparative Law Methods in the United States' (1998) 16 Roger Williams University Law Review 134, 134.

[117] Roux, 'Judging the Quality of Legal Research: A Qualified Response to the Demand for Greater Methodological Rigour' (n 112) 194.

[118] Ibid 194.

[119] See John C Reitz, 'How To Do Comparative Law' (1998) 46 American Journal of Comparative Law 617, 620; Konrad Zweigert and Hein Kotz, *Introduction to Comparative Law* (3rd revised edn, Clarendon Press 1998) 4.

[120] Zweigert and Kotz, *Introduction to Comparative Law* (n 119) 5.

[121] Roux, 'Judging the Quality of Legal Research: A Qualified Response to the Demand for Greater Methodological Rigour' (n 112) 194.

instrument to illuminate the analysis of Australian laws,[122] and is not concerned with the comparison of other jurisdictions for the sake of comparison. The approach is unabashedly utilitarian[123] and primarily intended to provide more material for the analysis of the legal problems likely to be of concern in Australia in relation to eObjects. It does not attempt to provide any deeper or larger analysis of patterns or themes across jurisdictions. Therefore, the approach taken in gathering comparative material and analysing that material was focussed on that purpose.

Comparative legal research is useful, even in this narrow form, 'simply because the different systems of the world can offer a greater variety of solutions than could be thought up in a lifetime by even the most imaginative jurist who was corralled in his own system'.[124] Aside from the comparison itself, the analytical tools used are similar to those employed in standard, non-comparative doctrinal research, such as a requirement to focus on all sources of law, including statute, cases and academic commentary.[125]

However, even in narrowly focussed comparative research, scholars must exercise particular comparativist skills when examining (as all comparative studies must) the similarities and differences between compared jurisdictions. With any comparative research, researchers must bear in mind that the *nature* of the legal problems in the different jurisdictions examined is likely to be different. Each legal system has its own language, intent and values which underlie its law. These reflect the 'the political, social and

[122] Ibid. See also Reitz, 'How To Do Comparative Law' (n 119) 620; Edward J Eberle, 'The Methodology of Comparative Law' (2011) 16 Roger Williams University Law Review 51, 51.

[123] In contrast to commentators such as Mark Van Hoecke and Mark Warrington, 'Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative Law' (1998) 47 ICLQ 495.

[124] Zweigert and Kotz, *Introduction to Comparative Law* (n 119) 15. See also Eberle, 'The Methodology of Comparative Law' (n 122) 51–52.

[125] Reitz, 'How To Do Comparative Law' (n 119) 628ff.

economic conditions of a particular jurisdiction'.[126] In research exploring sociotechnical change, technological conditions must also be added to this list. Differences in these conditions may have an effect on the utility of legal comparisons. Many information technologies, eObjects included, are not the same worldwide. They differ across jurisdictions, industries and organisations. These differences manifest themselves not only in their technical characteristics, such as their design and implementation, but also in the 'technological frame' through which people view them: the 'underlying assumptions, expectations and knowledge of particular technologies'.[127] The technological frame used is likely to have a consequential effect on how people choose to design, develop and interact with eObjects, and indeed, whether they choose to engage with them at all.

5.3 The specific nature of the research

The research involved documentary analysis of cases, legislation and commentary by academics; legal practitioners; consumer, industry and government organisations; journalists; bloggers; and commercial entities. The documentary analysis was not confined to scholarly legal literature and primary law sources. It included a significant amount of scholarly and popular literature in computer science and information systems, as well as scholarly literature in marketing, critical media studies and behavioural economics.

The research undertaken for this dissertation consisted of a number of steps. The author of this dissertation:

[126] Manoj Dias-Abey, 'Balancing Employee Protection with Promoting Business Productivity during Organisational Restructuring' (Masters thesis, University of New South Wales 2012) 27–28.

[127] Wanda J Orlikowski and Debra C Gash, 'Technological Frames: Making Sense of Information Technology in Organisations' (1994) 12 ACM Transactions on Information Systems 174, 174. See also Wiebe E Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (MIT Press 1995).

a) collected and reviewed a large number of industry publications relating to the technologies under consideration, including product announcements, reviews and media reports; and

b) conducted a literature review of the scholarly technical literature, and the existing legal literature.

Using the results of steps (a) and (b) above, the author of this dissertation then:

c) abstracted and analysed the attributes of, and interactions among, the technologies at issue. Those that are definitional were distinguished from those that are contributory. A unifying concept was invented and defined: the 'eObject' (the '**technical research framework**'); and

d) used the technical research framework to create a series of Vignettes illustrating the new things, activities and relationships enabled by eObjects and the systems in which they participate.

To provide a focus for the legal analysis, a conceptual framework was developed and adopted as set out in **Chapter 3**. Based on this conceptual framework, the author of this dissertation:

e) examined the attributes and interactions in the technical research framework and systematically identified where new things, activities or relationships might lead to challenges whose outcomes conflict with the goals of Australian law regulating consumer contracts, and therefore potentially give rise to legal problems;

f) identified one area of particular concern from step (e) above – a concept called 'digital consumer manipulation' in this dissertation – and using 'deductive … legal reasoning' as typically employed in doctrinal research,[128] analysed existing cases, legislation and commentary in the light of the conceptual framework and technical research framework to establish whether legal problems existed; and

[128] Margaret McKerchar, *Design and Conduct of Research in Tax, Law and Accounting* (Thomson Reuters/Lawbook Co 2010) 115.

g) outlined and analysed some potential solutions to the legal problems identified in step (f) above, using lessons learned from an examination of the conceptual framework.

Figure 1 provides a diagrammatic representation of the research approach set out in **sections 5.3(a)–(f)** above. It also sets out the boundaries of the broad and deep approach set out in **section 3.3** of this chapter, and delineates the areas of original contribution set out in **section 4.2** of this chapter (in the green shapes).

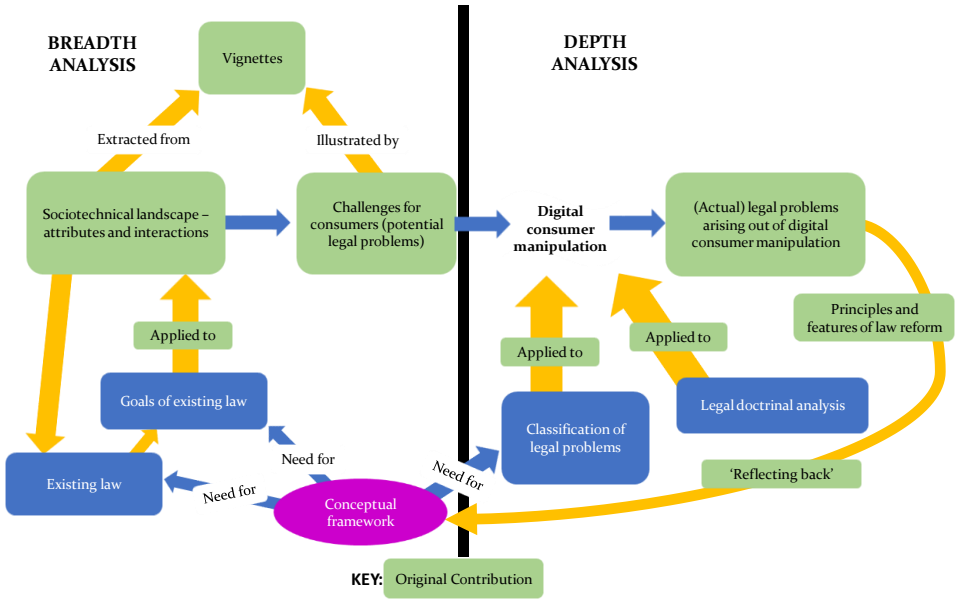

Figure 1: The research approach

5.4 Exclusions from scope

This dissertation talks about eObjects at a reasonably high level of abstraction. The level of abstraction chosen and possible alternatives are discussed in more detail in **section 2** of **Chapter 2**. The avenues for relevant research in the legal sphere are numerous. Research could concentrate on particular industries, such as home automation or driverless cars, or particular attributes of eObjects, such as active capacity (the ability of an eObject to act on the physical world). As a result of this richness, the scope (or *frame*, as discussed in **section 2.1.4** of **Chapter 3**) of this dissertation must be carefully defined. This section details the main exclusions from the scope of this dissertation, which include exclusions based on:

1) particular attributes of the technology, or its actual and potential use;
2) the multitude of challenges for consumers in relation to eObjects and ecommerce generally; and
3) the areas of law and the jurisdictions considered.

There are other, less significant exclusions from scope that are discussed at relevant places throughout the dissertation.

5.4.1 Attributes of eObjects

The scope of the technology at issue is thoroughly discussed in **Chapter 2.** However, one particular omission needs to be directly addressed. This dissertation does not use the term 'artificial intelligence' (or '**AI**'). This term is well over 60 years old, but still lacks an accepted definition.[129] The reason for the non-inclusion of the term in this dissertation is twofold. First, the concept of artificial intelligence is complex and contested,[130] and would require a dissertation (or multiple dissertations) on its own. Second, the realisation of this concept in real-life technological developments is still speculative, at least on some definitions of the term.[131]

However, some eObjects (or systems that incorporate them) exhibit a degree of *autonomy* in relation to decision-making and/or action. The attribute of autonomy is included within the scope of the dissertation. However, this is irrespective of whether it is achieved by a component or process (such as machine learning) that some would consider an expression of AI.[132]

---

[129] Iria Giuffrida, Fredric Lederer and Nicolas Vermeys, 'A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law' (2018) 68 Case Western Reserve Law Review 747, 753.

[130] For example, Toby Walsh, *It's Alive! Artificial Intelligence from the Logic Piano to Killer Robots* (La Trobe UP 2017) 17; House of Lords Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (Report of Session 2017–19, HL Paper 100, 16 April 2018) 13–14; Giuffrida, Lederer and Vermeys, 'A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law' (n 129) 753; Roger Clarke, 'What Drones Inherit from Their Ancestors' (2014) 30 Computer Law & Security Review 247, 249.

[131] Clarke, 'What Drones Inherit from Their Ancestors' (n 130) 248–51.

[132] Giuffrida, Lederer and Vermeys, 'A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law' (n 129) 753.

Therefore, **Chapters 3** and **5** of this dissertation will discuss the implications of eObjects and systems with some form of autonomy.

5.4.2 Challenges for consumers

Additionally, this dissertation does not discuss in any detail legal problems arising out of the new things, activities and relationships made possible by 'conventional' ecommerce. This dissertation is confined to a discussion of legal problems that arise particularly in the context of the sale and purchase of eObjects and systems, and where marketing, selling and buying is carried out by means of eObjects and systems.

Chapter 5 of this dissertation sets out areas where it is likely that consumers will suffer some sort of harm arising out of eObjects and the systems in which they participate. The multitude of consumer challenges identified in those chapters makes it impossible within the scope of this dissertation to identify all of the legal problems that might arise in Australia concerning those challenges. Consequently, a detailed analysis of the legislation and cases has been undertaken in relation to only one of those challenges: that of 'digital consumer manipulation'. Many, if not all, of the other challenges identified in **Chapter 5** remain fruitful subjects for further research and analysis of the specific nature of the legal problems that might arise. **Section 3.1** of **Chapter 8** sets out those challenges that should arguably be the highest priority for further research.

5.4.3 Legal exclusions

The scope of the doctrinal research in this dissertation is confined to a subset of the consumer protection law dealing with consumer contracts currently in force in Australia. Predominantly, the doctrinal analysis has been based on Schedule 2 of the Competition and Consumer Act 2010 (Cth) (**CCA**), known as the Australian Consumer Law, referred to as the 'ACL' in this dissertation. This dissertation examines the legislative principles contained in the ACL, and the associated case law. Additionally, it examines the common law of contract, and equitable principles where they affect the common law, in areas relating to consumers entering into contractual relationships.

Significant challenges for consumers arise out of data being collected, processed and distributed by eObjects, as discussed in **Chapter 5** (although it is important to note that not all of the challenges are data-related). The importance of data is also emphasised in **Chapter 6,** which discusses, in depth, the legal problems with using data to manipulate consumers into making purchases. In Australia, potential misuse of consumer data is usually seen as falling under the remit of the Privacy Act 1998 (Cth) (**Privacy Act**). This dissertation does *not* contain a detailed examination of the substantive provisions of the Privacy Act. This omission requires some explanation, which is set out in **section 3.5.1** of **Chapter 6**.

This dissertation does not analyse the impact of laws relating to the potential use of eObjects as surveillance devices. Surveillance activities may be hidden (such as the secret monitoring of Internet-connected toys) or ostensibly overt (such as visible cameras in public spaces). However, this dissertation does not consider the laws relating to government surveillance in Australia, such as the Surveillance Devices Act 2007 (NSW) (and other state equivalents) or the Surveillance Devices Act 2004 (Cth). Nor does it consider the surveillance of employees, which is regulated under the Workplace Surveillance Act 2005 (NSW) (and other state equivalents). As discussed in **section 3.4** of this chapter, this dissertation is restricted to the protection of citizens as 'consumers': that is, in some actual or potential commercial relationship with the providers of eObjects, the systems in which they participate, and associated services. It does not discuss in detail the legal problems that arise for individuals who are interacting with eObjects in a non-consumer or employee role. While not further discussed in this dissertation, since many eObjects incorporate telecommunications technologies, the reader should be aware of the potential effect of the Telecommunications (Interception and Access) Act 1979 (Cth). This Act contains a criminal offence of interception of private telecommunications

without the participants' knowledge by any person,[133] although it contains many exceptions.[134]

The comparative aspects of this research may have been enriched by examination of other countries in Asia with significant public and private investment in eObjects, such as South Korea[135] and China.[136] However, the author of this dissertation lacks familiarity with the native languages of these countries. This factor, combined with the paucity of relevant documents available in English, made the barriers to meaningful comparison too high to surmount. Accordingly, an examination of this kind was not attempted.

5.5 Keeping pace: legal and technical currency

Over the course of part-time doctoral study from 2013 to 2019, two key challenges needed to be addressed in order to complete this dissertation: (1) the pace of sociotechnical change; and (2) the substantial increase in interest by legal scholars in the particular area of law which is the subject of this dissertation during the period of candidature.

The significant probability of rapid sociotechnical change in this area over the course of part-time candidature in a doctoral program was apparent from the outset. Therefore, from the beginning of this research project, the approach to defining the sociotechnical landscape and the scope of the research was designed with this likelihood in mind. In defining the technology in **Chapter 2**, an attribute-based approach to the concept of eObjects is taken. The attributes are broadly defined in that chapter, which allows them to encapsulate a number of new technical approaches without becoming obsolete. Throughout the whole doctoral candidature period, time

[133] Telecommunications (Interception and Access) Act 1979 (Cth) s 7(1).

[134] For example, Telecommunications (Interception and Access) Act 1979 (Cth) s 7(2).

[135] Mellisa Tolentino, 'Most Influential Countries for the Internet of Things' (*siliconANGLE,* 21 March 2014) <http://siliconangle.com/blog/2014/03/21/most-influential-countries-for-the-internet-of-things/> accessed 2 June 2014.

[136] Maciej Kranz, 'What We Can Learn From China About IoT' (*Forbes*, 5 March 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/03/05/what-we-can-learn-from-china-about-iot/#36872d9237af> accessed 30 June 2018.

was set aside for periodic monitoring of technological developments. The author of this dissertation also regularly read a range of industry-based and scholarly technical literature to keep up to date with relevant sociotechnical change.

The upsurge in scholarly interest from 2016 onwards was less easy to predict, but not unexpected. Emerging scholarly debates on the subject were continually monitored, as was the legal practitioner literature. In terms of the literature review, the review of academic commentary in published journal articles was essential; however, the nature of the research area is such that waiting for published scholarly articles would have been inadequate. It was equally useful to monitor places where scholarly works-in-progress were advertised: in particular, working papers made available on public-access sites such as SSRN, and conference presentation and paper announcements made predominantly on social media sites such as Twitter and LinkedIn. To establish an original contribution to the scholarly debate in a timely manner, the author of this dissertation published four articles, and a peer-reviewed conference paper, over the course of doctoral candidature; these are now integrated into chapters of this dissertation. The research was also presented at two Australian and three international conferences.

Finally, part of the aim of the study is to discover the utility and possible limitations of the particular conceptual framework dealing with sociotechnical change adopted in this dissertation. As eObjects become more 'conventional', and legal problems are solved, the analysis of the *framework's* success (or otherwise) is likely to retain its utility well past the lifespan of the particular technology.

The case law and legislative materials on which this dissertation is based are current as of 30 June 2018. The *active* literature review of secondary materials was also completed on 30 June 2018, although a small number of references post-date this. Legal referencing style follows the Oxford University Standard

for the Citation of Legal Authorities (**OSCOLA**) 4th edition.[137] Where possible, case citations in the dissertation are neutral citations with pinpoint references to paragraphs. This is contrary to common practice in Australian law journals and legal texts, which prefer citations to pages in proprietary report series. However, this approach has been adopted in order to widen access to those readers who may not have access to increasingly expensive subscription services, and instead rely upon the freely available (but nevertheless high-quality) legal research services such as AustLII[138] that use the neutral citation system. The use of paragraph references also allows cited material to be more easily located, particularly where the reference is something other than a verbatim quotation from a judgment.

6 STRUCTURE OF THE DISSERTATION

Chapter 1 (this chapter) has outlined the research questions, the research approach and the significance and limitations of the research. **Chapter 2** sets out the nature of the technology facilitating the sociotechnical change under discussion, and develops a technical research framework of attributes and interactions. **Chapter 3** explains the conceptual framework used in this dissertation, introducing a categorisation of legal problems, and an approach to uncovering them in the face of sociotechnical change. As this framework requires identification of the goals of current laws applicable to the sociotechnical change being studied, **Chapter 3** proceeds to set out the goals of contract and consumer protection law that are relevant to consumer contracts. **Chapter 4** introduces a series of hypothetical Vignettes to assist in illustrating the types of legal problems that may arise out of the new things, activities and relationships made possible by eObjects. **Chapter 5** proceeds to apply the technical research framework set out in **Chapter 2,** and the Vignettes developed in **Chapter 4**, to identify and illustrate the main

[137] University of Oxford, Faculty of Law, *OSCOLA: The Oxford University Standard for Citation of Legal Authorities* (4th edn, Hart Publishing) <www.law.ox.ac.uk/sites/files/oxlaw/oscola_4th_edn_hart_2012.pdf> accessed 30 June 2018.

[138] Australian Legal Information Institute, 'AustLII' <www.austlii.edu.au/> accessed 30 June 2018.

challenges for consumers that arise out of these new things, activities and relationships. It does not identify *every* challenge for consumers. Rather, it identifies those challenges whose outcomes conflict with the goals identified in **Chapter 3**. **Chapter 6** discusses one of these challenges in depth, being that of digital consumer manipulation enabled by eObjects. That chapter analyses the current Australian consumer protection law to identify and categorise the legal problems that exist in relation to digital consumer manipulation: that is, where the existing law does not meet its goals. **Chapter 7** proposes principles and features that should be adopted in any attempts at law reform addressed at the legal problems identified in **Chapter 6**. **Chapter 8** provides a conclusion to the dissertation, setting out implications for further research and the lessons learned.

Chapter 2 – The sociotechnical landscape[139]

[139] This chapter reproduces substantial parts of a journal article published during the course of this doctoral study: Manwaring and Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (n 84). Also see n 1 for a discussion of authorship.

1 AIMS OF CHAPTER

> In order to craft appropriate laws, both the technology and its uses must be well understood.[140]

For the last 25 years, scholars, journalist and IT consultants, have been presaging what has been labelled the 'third wave of computing',[141] 'a new age of embedded, intuitive computing in which our homes, cars, stores, farms, and factories have the ability to think, sense, understand, and respond to our needs'.[142] Advocates of the third wave predict the large scale development and use of alternative forms of distributed information technologies. Early examples include smartphones, wearable computers and sensors and microprocessors embedded in everyday objects.[143] The aim of this chapter is to create an understanding of this third wave, and the new things, conduct and relationships it currently and potentially enables.

This third wave has led to different ways of doing business, different consumer experiences and different ways that humans interact with computer systems. It has also led to a plethora of technical literature on different aspects. However, up until the article in 2015 upon which this chapter is based, the *legal* literature generally failed to engage with the nature and features of the technology in a comprehensive way.[144] Much of

[140] Lyria Bennett Moses, 'Agents of Change: How the Law Copes with Technological Change' (2011) 20 Griffith Law Review 763, 786. This verbatim quote by Bennett Moses derives from ideas expressed by Chris Reed, 'Taking Sides on Technology Neutrality' (2007) 4 SCRIPTed 263, 282.

[141] Weiser, 'Ubiquitous Computing' (n 4).

[142] This reference to the 'third wave' is distinct from (although the choice of terminology may well have been inspired by) the description by futurist Alvin Toffler of first, second and third wave societies in Alvin Toffler, *The Third Wave* (Morrow 1980).

[143] Kalle Lyytinen and others, 'Surfing the Next Wave: Design and Implementation Challenges of Ubiquitous Computing' (2004) 30 Communications of the Association for Information Systems 695.

[144] With the notable exception of Anne Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (PhD thesis, University of Ottawa 2013). However, Uteck's

this has been deliberate. In the field of law, scholars have been approaching this question cautiously, feeling their way amongst discussions of technologies which are new, experimental and often merely visions of what 'might be' rather than actual applications in commercial use.

However, to develop more meaningful scholarship in how the law applies to this particular type of sociotechnical change, there needs to be a good understanding of the character of the technology at issue.[145] Even the early cautious approach taken by many legal scholars[146] assumes two things: a consistency in the technological literature concerning definitions and terminology; and a sufficient level of knowledge and understanding on the part of readers. The first assumption is unwarranted, and the second contentious. The technologies making up the 'third wave' have been called a number of different names, most commonly 'ubiquitous' and 'pervasive' computing, 'ambient intelligence', and the 'Internet of Things'. Unfortunately, both popular and academic writers have been inconsistent in their use of these terms. Definitions have varied depending on geographical locations, individual researchers, and have also changed over time.

This purpose of this chapter is to delineate the boundaries of the technologies being discussed in this dissertation, and to present a technical research framework designed to aid in the identification and analysis of

framework understandably focusses mainly on features of ubiquitous computing salient to her research on privacy, and therefore has some limitations for researchers looking at other issues.

[145] Reed, 'Taking Sides on Technology Neutrality' (n 140) 282; Mireille Hildebrandt, 'Law at a Crossroads: Losing the Thread or Regaining Control? The Collapse of Distance in Real-Time Computing' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010); Bert-Jaap Koops, 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010) 312.

[146] For example, Peppet, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (n 62); Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88); Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (n 61); Li, 'Deciphering Pervasive Computing: a Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' (n 55).

issues that might arise. A technical research framework is required in this dissertation to allow research in the area to proceed with a better understanding of the technological issues, and enable assessment of the capacity of existing law to deal with this new model of technology and its impacts on business and society.

The technical research framework developed in this chapter, along with the Vignettes developed in **Chapter 4**, is used in **Chapter 5** to analyse and illustrate key technical and functional innovations contained in the new model of computing brought about by the third wave. As discussed in **Chapter 3**, the identification of these innovations is required in order to uncover where legal problems may arise in relation to sociotechnical change.

2 THE NATURE OF THE TECHNOLOGY AT ISSUE

In any research investigating sociotechnical change, it is essential to clarify what technology is being discussed. Koops, in his 2010 analysis of mapping research spaces within law and technology regulation, argues that '[t]he questions raised by a certain development in technology depend very much on the character and level of abstraction of the technology at issue' (the '**technology type**').[147] Koops explains that questions of regulation will differ depending on whether a researcher is examining a concrete application of a certain technology (such as a fitness device), or more abstract notions such as information technology, or even technology, itself.

A technical research framework, reflecting the characteristics of the 'third wave', is presented in **section 4** of this chapter. However, it is also important to note at the outset that this description is the result of a deliberate choice to examine issues arising within a particular context. Various units of study exist, some of which are at differing levels of abstraction from one another, and others of which focus on particular features of the new model. For example, domotics (also known as home automation or 'smart homes') has

[147] Koops, 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' (n 145) 312.

been a popular and rapidly developing unit of study for computer scientists, designers, health professionals, consumer groups and policy bodies.[148] Domotics envisages the use of computers remotely controlling appliances and systems in the home such as security systems, climate control systems, audio-visual devices, lights, window coverings, and garden devices. In addition, significant research has been done on technical, social and legal implications of appliances,[149] wearables,[150] human ICT implants,[151] cyborgs,[152] augmented reality applications,[153] driverless cars,[154] marketing in mobile

[148] For example, M Meulendijk and others, 'AmI in Good Care? Developing Design Principles for Ambient Intelligent Domotics for Elderly' (2011) 36 Informatics for Health and Social Care 75; MM Kohn and others, 'SMART CAMP: Environmental Sustainability through Intelligent Automation Technologies' (24th IEEE International Conference on Advanced Information Networking and Applications, Perth, 20–23 April 2010); Rishabh Das and others, 'Security Based Domotics' (2013) 10 Procedia Technology 942; OECD, *Consumer Policy and the Smart Home* (n 67); Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63).

[149] Appliances in this context are computing devices whose full processing power is not made available to the end user, but is expressly constrained by the vendor to a small set of functionalities, for example Microsoft Xbox, Apple iOS devices, Amazon Kindle ebooks. See for example, Jonathan Zittrain, *The Future of the Internet and How to Stop It* (Yale UP 2008), particularly 101–26.

[150] For example, Steve Mann, 'Wearable Computing' in Mads Soegaard and Rikke Friis Dam (eds), *The Encyclopedia of Human-Computer Interaction* (2nd edn, The Interaction Design Foundation 2012).

[151] For example, Katina Michael and MG Michael (eds), *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies* (Advances in Human and Social Aspects of Technology, Information Science Reference 2014); Mark N Gasson, Eleni Kosta and Diana M Bowman, *Human ICT Implants: Technical, Legal and Ethical Considerations* (Information Technology and Law Series, Springer 2012).

[152] A cyborg can be defined as a 'human with whom mechanical and/or electronic parts have been integrated': Roger Clarke, 'Cyborg Rights' (2011) 30 IEEE Technology and Society Magazine 49, 50. See also Gowri Ramachandran, 'Against the Right to Bodily Integrity: Of Cyborgs and Human Rights' (2010) 87 Denver University Law Review 1.

[153] Augmented reality applications overlay additional digital information on images that are being viewed through a viewfinder on some form of computing device such as a smartphone. See for example the explanation in Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (n 61) 63–67.

[154] Maurice Schellekens, 'Self-Driving Cars and the Chilling Effect of Liability Law' (2015) 31 Computer Law & Security Review 506; Harry Surden and Mary-Anne Williams, 'Technological Opacity, Predictability, and Self-Driving Cars' (2016) 38 Cardozo Law Review 181.

health applications,[155] and artificial intelligence.[156] Researchers examining the technological developments described in this chapter may find it helpful to draw on the literature of these subsets and intersecting spaces, with an awareness that the differences in attributes and usage patterns will most likely affect the nature of the legal problems that might arise.

Multiple variants of the new model comprising the third wave have been described by academic and industry commentators, but not with consistency. The variants have been described in different terms, and with somewhat different characteristics. However, despite these varying descriptions, the major trend of the new model is the use of developments in information and communication technologies 'in order to enhance previously non-computerised everyday situations'.[157]

In more specific terms, the new model contemplates the widespread use of computer processors with data communications and data handling capabilities, embedded in a variety of objects from phones, to cars, to animals, to people. Some of these objects are new. One important feature of the new model, however, is that many of these objects previously existed, but were not previously capable of such communications and processes ('**enhanced objects**'). These enhanced objects may exist, operate and communicate in a fixed location, or with varying degrees of mobility. Importantly, mobile enhanced objects may be designed to be associated with human beings. They may be associated with an individual very closely (for example, subcutaneous chips, or chips in prostheses), loosely or episodically

[155] Nadine Bol, Natali Helberger and Julia CM Weert, 'Differences in Mobile Health App Use: A Source of New Digital Inequalities?' (2018) 34 The Information Society 183.

[156] For example, David C Vladeck, 'Machines Without Principals: Liability Rules and Artificial Intelligence' (2014) 89 Washington Law Review 117; Walsh, *It's Alive! Artificial Intelligence from the Logic Piano to Killer Robots* (n 130).

[157] Katharina E Kinder, 'Ubiquitous Computing in Industrial Workplaces: Cultural Logics and Theming in Use Contexts' (PhD thesis, Lancaster University 2009) 40.

(for example, phones, wearables such as spectacles or items of clothing), or very loosely (for example, cars).[158]

The new capabilities of these objects may be used for a wide variety of data collection, processing and dissemination purposes. This can occur through interactions with processors entrenched in conventional computing devices or in other new or enhanced objects. Discussions of the new model often concentrate on the potential benefits to individuals and organisations, as well as possible detrimental effects, such as a loss of control over personal data or decision-making. It should also be noted that much of the technical literature concentrates on technological possibilities, or as yet uncommercialised technology currently only found in research laboratories.

Section 3 of this chapter proceeds with an outline of the literature on historical and current definitions of particular areas of the new model. Beginning with the development of ideas of 'ubiquitous computing' in the early 1990s, **section 3** continues with a discussion of 'pervasive computing', 'mobile computing', 'ambient intelligence', and the 'Internet of Things', in order to provide a clear statement of the terminology and concepts behind the new model. This part also extracts from the literature some different ideas of the key dimensions or attributes of the new model. With considerable inconsistencies among existing analyses emerging, **section 4** of this chapter reconciles these analyses into a technical research framework and defines the technical scope of the dissertation.

3 DEFINITIONS: HISTORICAL AND CURRENT

The new model 'encompasses a wide range of disparate technological areas brought together by a common vision of computational resources deployed

[158] Although note that levels of association may vary between individuals; for example, some people may have much stronger emotional associations with their cars than their mobile phones.

in real-time, real-world environments."[159] Examples of concrete applications currently in commercial use or in advanced stages of development include:

- electricity smart grid technology;[160]
- wearable electronics and other consumer devices;[161]
- healthcare products;[162]
- home[163] and industrial[164] automation applications;

[159] Paul Dourish and Genevieve Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (MIT Press 2011) 61.

[160] For example, the Smart Grid, Smart City trials in New South Wales (see Australia, Department of Industry Innovation and Science, 'Smart Grid, Smart City' (n 13)), and similar trials in the US (see US Department of Energy Office of Electricity Delivery & Energy Reliability, 'Smartgrid.gov' (n 13), and the EU (European Commission Joint Research Centre, Smart Electricity Systems and Interoperability, 'Smart Grid Projects Outlook 2017' (n 13).

[161] For example, the Apple Watch, a wearable computer with smartphone-like functions (although currently somewhat limited and also dependent on proximity to a full-featured iPhone): see Apple, 'Choose the Apple Watch That's Right for You' <www.apple.com/au/shop/buy-watch/apple-watch> accessed 9 September 2018. Other examples include fitness trackers such as FitBit, Nike Fuelband and Jawbone.

[162] For example, Internet-connected insulin pumps: Jonah Comstock, 'Medtronic Launches Smartphone Connectivity for CGMs, Insulin Pumps' (*mobihealthnews*, 29 September 2015) <www.mobihealthnews.com/47112/medtronic-launches-smartphone-connectivity-for-cgms-insulin-pumps> accessed 26 March 2018. Technology for a general-purpose health monitoring device is still under development: Jo Best, 'Building the Tricorder: The Race to Create a Real-Life Star Trek Medical Scanner' (*ZDNet,* 26 November 2018) <www.zdnet.com/article/building-the-tricorder-the-race-to-create-a-real-life-star-trek-medical-scanner/> accessed 31 December 2018.

[163] For example, Internet-enabled light, energy, security, entertainment, appliances, water – see Turban and others, *Electronic commerce: a managerial and social networks perspective* (n 7) ch 6. For example, LG has released an Internet-enabled and voice- and smartphone-activated refrigerator which manages expiry dates, creates shopping lists, and sends recipes to the householder (and their oven) LG <www.lg.com/us/discover/smartthinq/refrigerators> accessed 5 September 2018. A Brazilian company currently markets the SmartHydro, a bath which can be filled remotely by communication with a smartphone, The Innovative House, 'SmartHydro' <www.ihouse.com.br/caracteristicas-da-smarthydro.php> accessed 27 August 2018.

[164] For example: wireless sensor networking products such as SmartMesh WirelessHART, Analog Devices, 'SmartMesh WirelessHART' (n 9); control systems in coal mines C. Zhou and others, 'Industrial Internet of Things (IIoT) applications in underground coal mines' (2017) 69 Mining Engineering 50; and validation of production records in pharmaceutical manufacturing, Caroline Hroncich, 'Integrating Industrial Internet of Things and Pharmaceutical Manufacturing Processes' (2017) 41 Pharmaceutical Technology 46.

- traffic applications;[165]
- smart and driverless cars and trucks;[166] and
- environmental monitoring.[167]

However, despite the fact that it is easy to point to current (and potential) examples, it is difficult to identify an accurate scope definition of this 'new model' of computing. The terminology used by researchers, industry participants and governments is not fixed, and a number of different terms are frequently used. The most commonly used terms appear to be **ubiquitous computing**,[168] **pervasive computing**,[169] **ambient intelligence**,[170] and the **Internet of Things**.[171] While other terms are also used, such as 'smart' technology,[172] cyber-physical systems[173] or 'everyware',[174] the first four listed in bold are by far the dominant terms. Sometimes these

[165] For example, traffic congestion reporting and automated decision-making services offered by Inrix <http://inrix.com/> accessed 9 September 2018.

[166] For example, Daimler 'Smart' brand cars, Google's driverless car, SARTRE self-driven road trains. See Turban and others, *Electronic commerce 2012: a managerial and social networks perspective* (n 10) 315–16.

[167] Oliveira and Rodrigues, 'Wireless Sensor Networks: a Survey on Environmental Monitoring' (n 15).

[168] Weiser, 'The Computer for the 21st Century' (n 19). Ubiquitous computing is also commonly abbreviated to 'ubicomp', the abbreviation appearing to have originated with Mark Weiser himself: the earliest reference found is to a penultimate draft of a paper published in *Scientific American* in 1991 (the term did not appear in the published article). The penultimate draft containing the abbreviation was originally available at <www.ubiq.com/hypertext/weiser/SciAmDraft3.html>, but some time post 24 June 2018 this website was taken down. A copy of the original draft from Google's cache has been retained by the author of this dissertation. This abbreviation has been used frequently since: most notably as the title of the Association for Computing Machinery's annual International Conference since 2001 – Ubicomp, 'Ubicomp 2018' <http://ubicomp.org/ubicomp2018/> accessed 9 September 2018.

[169] For example, Adelstein and others, *Fundamentals of Mobile and Pervasive Computing* (n 20).

[170] For example, Information Society and Technology Advisory Group, *Strategic orientations and priorities for IST in FP6* (n 21).

[171] For example, Gershenfeld, Krikorian and Cohen, 'The Internet of Things' (n 22).

[172] For example, Brenner, *Law in an Era of 'Smart' Technology* (n 57); Mireille Hildebrandt, *Smart technologies and the end(s) of law: novel entanglements of law and technology* (Edward Elgar Publishing 2015).

[173] For example, Stefano Zanero, 'Cyber-Physical Systems' (2017) 50 Computer 14.

[174] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (New Riders 2006).

terms are used interchangeably, other times they are used in different but overlapping contexts, with wider or narrower scopes of meaning.

This profusion and confusion of terms may be due to a number of reasons. Terminologies and descriptions in the literature appear to be contingent on a number of factors. They vary over geographical locations, between individual researchers, and change over time. In particular, terminology has often varied depending upon the particular entity funding the research being discussed. Also, whereas many areas of information technology research have a significant and defined technical problem or problems to be solved, the research arenas of ubiquitous computing, pervasive computing and ambient intelligence have a far greater focus on the human (rather than technical) outcomes.[175] As a result, a great breadth of technology types and technical problems come under the research umbrella of these areas. This breadth makes almost any attempt at definition 'messy', as Dourish and Bell characterise it.[176]

In order to come to a proper view of how the law does and should treat these emerging technologies, it is important to clear up at least some of the 'messiness', clarify the fields of view of the various terms, and identify the characteristics that are of greatest relevance to their impacts. It is also important to understand the way the law interacts with the products, services and relationships that arise from the use of these technology types.

3.1 Ubiquitous and pervasive computing

3.1.1 History

In 1991 and the years that followed, a computer science researcher, Mark Weiser, articulated a vision of a world where the traditional computer would be replaced by tiny devices. These devices would be distributed and

[175] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 61.
[176] Ibid.

embedded in items in the physical world, communicating and interoperating with each other with the benefit of new wireless communication technologies.[177] Weiser coined the term 'ubiquitous computing' for this pattern of computing use.[178]

Ubiquitous computing has not yet been fully implemented in 2018 – or at least not in the way Weiser imagined it.[179] However, much of the technology he visualised now exists either in research laboratories or has been fully commercialised, although with significant variations in business and consumer take-up. This has been facilitated by technological advances in:

> areas such as Internet technologies, mobile and distributed computing, handheld devices, computer hardware, wireless communication networks, embedded systems and computing, wireless sensor networks, software agents, human computer interfaces, and the like.[180]

Most attempts at a definition of the new model use Weiser's vision as a starting point, focusing 'on potential benefits of widely distributed input and output devices – sensors, effectors, and displays that will be carried, worn, or embedded in the environment.'[181]

Weiser's publications emerged from his research work as chief scientist at Xerox PARC, a research division of Xerox Corporation Ltd. In the early 1990s, however, a rival industrial vision emerged. IBM created a new research division which promoted research along the lines of leaving the desktop

[177] Weiser, 'The Computer for the 21st Century' (n 19); Mark Weiser, 'The World is not a Desktop' (1994) Interactions 7; Weiser and Brown, 'The Coming Age of Calm Technology' (n 6).

[178] Weiser, 'The Computer for the 21st Century' (n 19) 94.

[179] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) ch 2.

[180] Mohammad S Obaidat, Mieso Denko and Isaac Woungang (eds), *Pervasive Computing and Networking* (John Wiley & Sons 2011) 3. Of particular interest for ubiquitous computing are the developments in radio frequency identification and near field communication (NFC) protocols.

[181] Jonathan Grudin, 'Group Dynamics and Ubiquitous Computing' (2002) 45 Communications of the ACM 74, 74.

computer behind in order to develop opportunities in mobile and embedded computing. At this time, IBM developed a 'architecture and marketing concept' that they labelled 'pervasive computing'.[182]

The two terms seemed to emerge as competing attempts from within two different organisations, Xerox PARC and IBM, both aimed at carving out a unique research space. However, from the beginning, there appeared to be a significant overlap in the two research foci of ubiquitous and pervasive computing. Want identified one major differentiation between the two research areas in the early 1990s: the emphasis by Xerox PARC on 'calm' and 'disappearing' technologies. This emphasis on invisible computing did not appear in IBM's early marketing efforts.[183]

In the next decade, some researchers explicitly attempted to differentiate the two terms. IBM had a common starting point with Xerox PARC in investigating opportunities in connected mobile and embedded computing.[184] However, in 2002 Lyytinen and Yoo distinguished the two terms as set out in **Table 1**.

Table 1: Comparison of pervasive and ubiquitous computing

Type of computing	Level of mobility	Level of embeddedness
Pervasive computing	Low	High
Ubiquitous computing	High	High

They argued that 'the main challenges in ubiquitous computing originate[d] from integrating large-scale mobility with the pervasive computing functionality'. In other words, design challenges arose out of the desire by

[182] Sandhu Reema, 'Shifting Paradigm from Mobile to Ubiquitous/Pervasive Computing' (2013) 2 COMPUSOFT: International Journal of Advanced Computer Technology 360, 360.

[183] Roy Want, 'An Introduction to Ubiquitous Computing' in John Krumm (ed), *Ubiquitous Computing Fundamentals* (Chapman & Hall/CRC 2009) 10.

[184] Ibid 11.

developers for computers to retrieve information from their environment through interaction with other computing systems and act '"intelligently" upon and within the environments in which we move'.[185]

Therefore, a 'smart office' containing sensors and actuators[186] which sense a person entering and turn on lights, adjust heating and activate displays would be a good example of *pervasive* computing, within the Lyytinen and Yoo definition. The Sensoria smart sock[187] would provide a better example of *ubiquitous* computing. The manufacturers have sewn a sensor chip into socks, which can communicate with a smartphone app. The sensor chip sends information about the wearer's running style to the smartphone app; the app itself sends alerts to the runner's mobile phone when, for example, the runner's tendency to heel strike exceeds acceptable levels.[188] This type of computing is both embedded and highly mobile. Personal medical devices such as Internet-connected insulin pumps and glucose monitors[189] also provide good examples of ubiquitous computing.

However, even before Lyytinen and Yoo's article, commentators tended to conflate the two concepts,[190] and the differences began disappearing. Singh, Puradkar and Lee in 2006 attempted to stop the convergence of the two definitions, stating that they were 'conceptually different'. However, even in their description of the two these authors co-opted the concept of

[185] Kalle Lyytinen and Youngjin Yoo, 'Issues and Challenges in Ubiquitous Computing' (2002) 45 Communications of the ACM 62, 64.

[186] Actuators are devices that move things.

[187] Sensoria <www.sensoriafitness.com/> accessed 10 September 2018.

[188] Will Oremus, 'Smart socks may be the future of wearable technology' *The Sydney Morning Herald* (Sydney, 30 November 2013) <www.smh.com.au/digital-life/digital-life-news/smart-socks-may-be-the-future-of-wearable-technology-20131130-2yihx.html>.

[189] Comstock, 'Medtronic Launches Smartphone Connectivity for CGMs, Insulin Pumps' (n 162). See also Medtronic <www.medtronic-diabetes.com.au> accessed 23 August 2018.

[190] For example, Mahadev Satyanarayanan, 'Pervasive Computing: Vision and Challenges' (2001) 8 IEEE Personal Communications 10, 10 ('*ubiquitous computing*, now also called pervasive computing'). See also D Saha and A Mukherjee, 'Pervasive Computing: A Paradigm for the 21st Century' (2003) 36 Computer 25.

invisibility into *pervasive* computing:[191] a concept that had been fundamental to the early descriptions of *ubiquitous* computing by Weiser.

It appears, however, that Singh, Puradkar and Lee were fighting a losing battle. From the mid-2000s or even earlier, most authors displayed a tendency to use both terms interchangeably or else acknowledge significant overlaps.[192] Some relatively recent work still attempts to differentiate the two[193] but Want, writing in 2010, argued that 'any unique position described by either party has been slowly integrated into the shared vision and by the mid-2000s any publications that set out to describe this topic presented fundamentally the same position'.[194] By this time, the number and diversity of actors involved in the field may well have meant that the convergence of the terms, considering their real similarities, was almost inevitable.[195]

[191] Sachin Singh, Sushil Puradkar and Yugyung Lee, 'Ubiquitous Computing: Connecting Pervasive Computing through Semantic Web' (2006) 4 Information Systems and e-Business Management 421, 422.

[192] See for example, Adelstein and others, *Fundamentals of Mobile and Pervasive Computing* (n 20) 92 ('Since the mid-1990s, ubiquitous computing has also been known as *pervasive computing*'); George F Coulouris and others, *Distributed Systems: Concepts and Design* (Addison-Wesley 2012) 819 ('Ubiquitous computing is also sometimes known as pervasive computing, and the two terms are usually taken to be synonymous'); Stefan Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (John Wiley & Sons Ltd 2009) xxv ('Ubiquitous Computing, often also referred to as Pervasive Computing'); Uwe Hansmann, *Pervasive Computing: The Mobile World* (2nd edn, Springer 2003) 1 ('"*Everywhere at anytime*' … This common slogan expresses in a nutshell the goal of Pervasive or Ubiquitous Computing').

[193] For example, Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Sage 2014) 84 ('If the mantra of pervasive computing is computation "in everything", then the mantra of ubiquitous computing is computation "in every place", with pervasive computing exhibiting processes of divergence (software being embedded into more and more devices) and ubiquitous computing exhibiting convergence (single digital devices undertaking more and more tasks)'). See also Rob Kitchin and Martin Dodge, *Code/Space: Software and Everyday Life* (MIT Press 2011).

[194] Want, 'An Introduction to Ubiquitous Computing' (n 183) 11.

[195] One significant indicator of convergence was the 2013 merger of the Association for Computing Machinery's two separate international conferences on pervasive and ubiquitous computing into one – UbiComp. See Association for Computing Machinery, 'UbiComp 2013' <www.ubicomp.org/ubicomp2013/index.php> accessed 20 June 2018.

3.1.2 Properties of ubiquitous computing

In 1991 Weiser identified the main properties of ubiquitous computing as being computing that was **distributed**, **unobtrusive** and **context-aware**.[196] He also identified three form factors for potential ubiquitous computing devices, then being researched in the Xerox PARC laboratories: 'tabs', 'pads' and 'boards'.[197] Notably, modified versions of these form factors have become an intrinsic part of common technologies commercially available in 2015 (as smartphones, tablets and interactive whiteboards respectively), even though their usage is not quite as 'ubiquitous' as Weiser might have hoped. In 2005, Endres, Butz and Macwilliams took a more expansive systems approach, and classified ubiquitous computing systems into three broad areas: augmented reality (virtual layer on a physical environment); intelligent environments (embedded sensors, actuators and/or processors); and distributed mobile systems (integrated multiple mobile devices).[198]

The most comprehensive framework proposed for ubiquitous computing was one developed by Poslad in 2009. He identified a three-pronged framework for technical analysis and design of ubiquitous computing systems, called SmartDEI. Although Poslad called his book 'Ubiquitous Computing', he made it clear that he included concepts of pervasive computing and ambient intelligence within that term.[199]

Poslad undertook a substantive literature review of authors who had identified a number of different types of classifications based on functional properties, types of devices, and types of systems.[200] From this review, he identified five 'core internal properties' (and over 70 sub-properties) that

[196] Weiser, 'The Computer for the 21st Century' (n 19) 94–95, 98–102, 104.

[197] Ibid 98.

[198] Christoph Endres, Andreas Butz and Asa MacWilliams, 'A Survey of Software Infrastructures and Frameworks for Ubiquitous Computing' (2005) 1 Mobile Information Systems 41, 42.

[199] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 18.

[200] Ibid 17–18.

ubiquitous computing devices and systems should manifest. He considered these core properties to be:

1) **distributed** systems which are **networked** and **transparent** ie 'acting as a single virtual system even though it is physically distributed'.[201] Poslad uses the term 'transparency' consistently throughout his work to designate a desired design outcome of 'hid[ing] the complexity of the distributed computing model from users'.[202] This is a problematic term. Other writers use this term in relation to Weiser's idea of a 'disappearing' or non-obtrusive computer,[203] which Poslad puts into his second category. From the perspective of a user (or usee), Poslad's use of 'transparency' would probably be better phrased as 'opaqueness' or a 'black box' approach to design;

2) the interaction between humans and computing devices/systems is **implicit**, or at least less obtrusive than conventional desktop computers. (Note the physical size of the computer device, or the object into which it is embedded, may be quite large, but the interaction may be much less obvious.) Poslad labelled the more extreme versions of this implicit human-computer interaction, or '**iHCI**';[204]

3) computers are **context-aware** – of the physical environment, users and other computing systems;

[201] Ibid 19.

[202] Ibid 8.

[203] DJ Cook, JC Augusto and VR Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (2009) 5 Pervasive and Mobile Computing 277, 279; Coulouris and others, *Distributed Systems: Concepts and Design* (n 192) 10.

[204] Poslad adopted the terminology from Albrecht Schmidt, 'Implicit Human Computer Interaction through Context' (2000) 4 Personal Technologies 191, who further developed this in Albrecht Schmidt, 'Ubiquitous Computing: Computing in Context' (PhD thesis, Lancaster University 2002).

4) computers can operate **autonomously** (ie devices/systems can be 'self-governing and are capable of their own independent decisions and actions'); and

5) computers deal with multiple actions and interactions via '**intelligent**' decision making and interaction systems. Poslad indicates this concept 'may entail some form of artificial intelligence'.[205]

As Poslad's framework provides a useful checklist of features found in 'third wave' technologies, this dissertation contains a summary of Poslad's list of properties and sub-properties in **Table 5** in **Appendix A**.

Poslad concluded from his review that no one definition of ubiquitous computing was possible, and 'rather there is a range of properties and types … which vary according to the application'.[206] He proposed a fluid classification where 'each individual property has its own domain of a more finely grained set of discrete values, rather than being seen as a property that is present or absent'.[207] Therefore, an individual system could display some but not all of the core properties strongly, and the remaining only weakly or perhaps not at all. From a definitional perspective, there are two significant problems with Poslad's classification of 'core properties'. The first is that many of the properties that he describes are not core at all. It seems he uses the term as indicating 'possible' properties, rather than requiring these properties as part of a definition exercise. Also, when he attempts to define these core properties, the endpoints of the dimensions are not sufficiently described.

The second part of Poslad's framework focussed on design architectures seen in ubiquitous computing systems. Poslad expanded on the previous ideas of Satyanarayanan[208] to identify three types of design architectures: 'smart

[205] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 9. The first three of these are explicitly adapted from Weiser's work; the last two were additional proposals from Poslad.

[206] Ibid 35.

[207] Ibid 21.

[208] Satyanarayanan, 'Pervasive Computing: Vision and Challenges' (n 190).

device', 'smart environment', and 'smart interaction'. Smart devices in Poslad's framework take a range of forms, but are most often **multi-functional**, **personal** devices such as mobile phones. They have a large amount of **explicit** interaction with humans, and between the device and other computers, but less so with the physical environment. Smart environments, by contrast, tend to contain **embedded** devices which are more limited in functionality,[209] but support higher levels of **implicit** human-computer interaction. For example, a door-opening system which opens a door automatically when a human approaches has only one function, but can be used without complex thought or action by a human. Smart environments also tend to be more **public** than personal as they usually support interactions with many users.

Smart interaction systems were defined as a further step on from basic synchronous and asynchronous interactions between a sender and receiver, involving the use of both personal smart devices and smart environments. For example, Poslad's idea of smart interaction contemplated that a choice of action by a device (such as switching on a light, or rather a particular light in the room) will be dependent on sharing and processing information about

[209] See the explanation of 'appliances' in n 149. 'Embedded' components can be embedded in parts of a physical or human environment, or be part of a larger ICT device. 'Untethered' components are those that have some degree of physical freedom. These untethered components are likely to include micro electromechanical systems (MEMS) devices, often referred to as 'smart dust'. Current MEMS products include automotive pressure sensors, airbag accelerometers and inkjet heads (although most growth is expected from MEMS technologies that are still early in the research and development stage): AA Berlin and KJ Gabriel, 'Distributed MEMS: New Challenges for Computation' (1997) 4 IEEE Computational Science and Engineering 12. Poslad, when discussing smart environments, concentrates on future possible uses of MEMS devices, such as a series of micro-sensors applied over surfaces, or diffused through other liquid or gaseous materials. For example, he raises the possibility that 'smart paint' might be developed for transport infrastructure containing sensors which track traffic, wind and structural integrity: Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 197.

user goals (for example, whether or not the user is reading a book or watching a film).[210]

Poslad also viewed third wave systems through a third lens, based on the type of **external interaction** inherent in ubiquitous computing systems. Poslad considered that there were three basic ubiquitous computing systems environments: the virtual (other ICT systems), the physical, and the human. The external interactions comprise human-to-computer, computer-to-physical world and computer-to-computer interactions, as well as combinations and reversals of these. For example, a human playing a game on a smartphone incorporates a human-to-computer interaction. Computer-to-computer interaction is required if the game is one with multiple remote players. Physical world-to-computer interaction will also be required if the game contains augmented reality features, such as Niantic Labs' Ingress and Pokémon Go. These games are GPS-dependent, and require users to be within a certain physical distance of physical landmarks in order to perform certain actions within the game.[211]

3.2 Mobile computing

Contemplating the use of a smartphone or other mobile device as part of a ubiquitous computing system brings added complexity to a definition of the new model described in this chapter. This complexity results from the rise and dominance of mobile computing in the modern information technology landscape, most obviously demonstrated by the runaway commercial success of mobile phones with significant computer processing power. Mobile computing can be described as 'the performance of computing tasks while

[210] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 33. Note that this particular scenario has not yet been realised; its utility will, in all likelihood, be limited by factors such as the need for human intention to produce some phenomenon that can actually be sensed by a machine.

[211] Ingress <www.ingress.com> accessed 9 September 2018; Pokemon Go <www.pokemongo.com> accessed 9 September 2018.

the user is on the move, or visiting places other than their usual environment.'[212]

The increasing use of smartphones and wireless tablets in developed and developing economies is one of the most obvious examples of the 'third wave', or the move away from the desktop model. However, it is arguable that mobile computing is not confined to mobile phones and tablets. The concept could also cover areas such as wearable computing,[213] for example Internet-connected spectacles,[214] or computing which is implanted in humans or other animals, such as a heart pacemaker.[215]

However, significant distinctions between mobile computing and Weiser's initial view of ubiquitous computing have previously been identified.[216] For one:

> [b]roadly speaking, mobile computing is concerned with exploiting the connectedness of devices that *move around* in the everyday physical world; ubiquitous computing is about exploring the

[212] Coulouris and others, *Distributed Systems: Concepts and Design* (n 192) 10.

[213] For a discussion of the history of wearable computing, see Mann, 'Wearable Computing' (n 150).

[214] Such as Google Glass, Sony's Smart Eyeglass, and Toshiba's dynaEdge™ AR Smart Glasses. Consumer use of Internet glasses has been problematic, particular due to privacy concerns: see Paul Briden, 'Google Glass Review: Glass in Its Current Form is Dead' (*Know Your Mobile,* 11 April 2014) <www.knowyourmobile.com/google/google-glass/21388/google-glass-release-date-features-and-price-ray-ban-oakley-commit-future> accessed 13 June 2018; Gene Marks, 'How Google Saved Google Glass' (*Forbes*, 2 February 2012) <www.forbes.com/sites/quickerbettertech/2015/02/02/how-google-saved-google-glass/> accessed 4 February 2015. However, some significant business applications have been developed. See Tom Simonite, 'Google Glass is Back: Now with Artificial Intelligence' (*Wired*, 25 July 2018) <www.wired.com/story/google-glass-is-backnow-with-artificial-intelligence/> accessed 25 July 2018; Dynabook, 'dynaEdge™ AR Smart Glasses' <https://smartglasses.toshiba.com/> accessed 8 January 2019.

[215] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 29.

[216] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 117.

> increasing integration of computing devices *with[in]* our everyday world.[217]

Another important distinction arises from the nature of the interaction between device and user. Ubiquitous computing from the beginning contemplated a user model with many different computers (each often with only one or two dedicated functions) interacting with many different users, or with different machines or devices. Mobile computing, on the other hand, currently operates closer to the desktop model. A user interacts directly with one or two devices dedicated to her or him. Also, discussions of mobile computing usually assume a human's central involvement in the computing activity, while ubiquitous/pervasive computing does not confine itself in this way.

However, apart from these distinctions, mobile computing seems entrenched as part of the research space of ubiquitous/pervasive computing. Its features are usually discussed by computer scientists and other researchers as an essential part of ubiquitous computing concepts, whether as a subset or as a necessary adjunct.[218] In 1996, Weiser himself denied that ubiquitous computing was either a 'superset or subset' of mobile computing,[219] but it is unlikely that this position can continue to be justified considering the technological and terminological changes since that time. For example, Weiser specifically rejected the idea of his vision of ubiquitous computing 'liv[ing] on a personal device of any sort', but rather contemplated it existing 'in the woodwork everywhere'.[220] However, the 'tabs' and 'pads' prototypes he helped Xerox PARC develop have now been transformed into *personal* devices, predominantly smartphones and tablets. The mobile infrastructure

[217] Coulouris and others, *Distributed Systems: Concepts and Design* (n 192) 818 (emphasis added).

[218] See for example, Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192); Adelstein and others, *Fundamentals of Mobile and Pervasive Computing* (n 20); Coulouris and others, *Distributed Systems: Concepts and Design* (n 192); Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159).

[219] Weiser, 'Ubiquitous Computing' (n 4).

[220] Ibid.

essential to the commercial success of these personal devices could be seen as indeed embedded in the 'woodwork', admittedly not everywhere, but in very many places. Dourish and Bell in 2011 concluded that existing mobile computing is, in its own way, the current manifestation of Weiser's vision of ubiquitous computing, albeit messy, incomplete and using technologies in a way he had not anticipated.[221]

3.3 Ambient intelligence

3.3.1 History

The emergence of the term 'ambient intelligence' came almost a decade after the development of ubiquitous and pervasive computing. It was first used in 1998 in a series of workshops commissioned by consumer electronics company Philips.[222] By 2009, the fundamental idea of 'ambient intelligence' was defined as:

> by enriching an environment with technology (for example, sensors and devices interconnected through a network), a system can be built … which senses features of the users and their environment, then reasons about the accumulated data, and finally selects actions to take that will benefit the users in the environment.[223]

Note that the idea of 'benefits' in this definition was specifically related to 'the users in the environment'. The authors also identified loss of control, privacy and security concerns as possible disbenefits of these technologies.[224]

Philips spearheaded the corporate development of the concept, also developing links with industries and research universities, such as its

[221] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 24–26.

[222] EHL Aarts and José Luis Encarnação (eds), *True Visions: The Emergence of Ambient Intelligence* (Springer-Verlag 2006) 6.

[223] Cook, Augusto and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (n 203) 278.

[224] Ibid 286–87.

collaboration with the MIT Oxygen project,[225] and its in-house development of a research laboratory to investigate scenarios for ambient intelligence, HomeLab.[226] The Philips workshops identified some particular characteristics of ambient intelligence, including that the technology used would be **embedded**, **personalised**, **adaptive** and **anticipatory**.[227]

The idea – and the terminology – of ambient intelligence were given their most significant boost as a result of substantial investment by the EU. In 1999, the EU's Information Society and Technology Advisory Group (**ISTAG**) created a workgroup on 'Ambient Intelligence', and issued a series of reports over the next couple of years.[228] As a result of ISTAG's recommendations, ambient intelligence research formed a key part of the European Commission's Sixth Framework Programme for Research and Technological Development in the area of Information Society Technologies.[229] In its first report, ISTAG postulated four different scenarios concerning possible development in ambient intelligence technologies. One scenario described a woman who lived in a 'smart house' where she could order food and other items via her refrigerator, and track her e-commerce activities via a mobile device. She could also access a carpool through her city infrastructure, which

[225] MIT Project Oxygen, *Pervasive, Human-Centred Computing* <oxygen.lcs.mit.edu/> accessed 28 August 2018.

[226] Noldus, 'Philips HomeLab' <www.noldus.com/default/philips-homelab> accessed 9 September 2018.

[227] Eli Zelkha and Brian Epstein, 'From Devices to "Ambient Intelligence": The Transformation of Consumer Electronics' (Presentation slides circulated internally within Royal Philips Electronics, 24 June 1998) <www.epstein.org/brian/ambient_intelligence.htm> accessed 25 February 2012.

[228] Information Society and Technology Advisory Group, *Scenarios for Ambient Intelligence in 2010* (Final Report, European Commission Community Research, 2001); Information Society and Technology Advisory Group, *Strategic Orientations and Priorities for IST in FP6* (n 21); Information Society and Technology Advisory Group, *Ambient Intelligence: From Vision to Reality* (Report, European Commission, September 2003).

[229] European Parliament and European Council, Decision No 1513/2002/EC of the European Parliament and of the Council of 27 June 2002 concerning the sixth framework programme of the European Community for research, technological development and demonstration activities, contributing to the creation of the European Research Area and to innovation (2002 to 2006).

would also advise on traffic and also regulate the car's behaviour accordingly.[230]

3.3.2 Characteristics of ambient intelligence

It is noteworthy that, like the terms 'ubiquitous' and 'pervasive' computing, the term 'ambient intelligence' emerged from a separate research organisation. The 2009 definition above makes clear the similarities between the scope of ambient intelligence and ubiquitous/pervasive computing research. However, unlike those terms, 'ambient intelligence' has in many cases maintained a separate identity,[231] most likely due to its adoption by the EU in 2001 and consequential funding of research projects. It still remains a predominantly European term. The question remains: are there important differences?

Some scholars have proposed that the key distinguishing feature of ambient intelligence, when compared to ubiquitous or pervasive computing, is the assertion that the technologies need to be intelligent, in some sense of that word.[232] The very name assumes that ambient intelligence research concentrates on devices acting intelligently, but the term often seems to be used functionally, rather than engaging with existing complex and contested definitions[233] of artificial or synthetic 'intelligence'. In particular, the term 'intelligence' is most often used in ambient intelligence literature as a synonym for making people's lives easier, which is difficult to justify as a defining factor.[234] Undoubtedly technologies exist that can collect large

[230] Information Society and Technology Advisory Group, *Scenarios for Ambient Intelligence in 2010* (n 228) 38–42.

[231] For example, with separate journals and conferences.

[232] E Maeda and Y Minami, 'Steps towards Ambient Intelligence' (2006) 4 NTT Technical Review 50, 51. See also Cook, Augusto and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (n 203) 279.

[233] A discussion of the complexity of the debate around definitions of artificial intelligence can be found at Clarke, 'What Drones Inherit from Their Ancestors' (n 130) 248–51.

[234] For example, M Friedewald and others, 'Perspectives of Ambient Intelligence in the Home Environment' (2005) 22 Telematics and Informatics 221, 222; G Riva and others, 'Presence 2010: The Emergence of Ambient Intelligence' in G Riva, F Davide

amounts of data, use strong contextual models to recognise a problem that needs to be solved, and contain clever algorithms which can suggest solutions. Whether or not this is sufficient to be called 'intelligent' is highly contested.[235] Aside from the outstanding question of whether technology can in fact ever approach human capabilities for flexibility, adaptability, tolerance and wisdom, an emphasis on intelligence alone as a *differentiating* factor is highly questionable considering the significance scholars have attributed to an 'intelligent response' in ubiquitous and pervasive computing.[236]

A more sensible attempt at differentiation was made by ISTAG. It saw ambient intelligence as being 'concerned less with basic technology than the use of the technology – by the individual, by business, and by the public sector.'[237] This was supported by Sorrano and Botia, who proposed that:

> Ubiquitous Computing … is a vision for computer systems to merge the physical world and human and social environments … And Ambient Intelligence … is concerned with such kind of systems but it lays the emphasis on how they interact with people'.[238]

---

and WA IJsselsteijn (eds), *Being There: Concepts, Effects and Measurements of User Presence in Synthetic Environments* (IOS Press 2003) 61.

[235] Clarke, 'What Drones Inherit from Their Ancestors' (n 130) 248–51.

[236] See Lyytinen and Yoo, 'Issues and Challenges in Ubiquitous Computing' (n 185) 64. See also particularly Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 18, who considered that ambient intelligence fit along a spectrum of types of ubiquitous computing, with an emphasis on autonomy, implicit human computer interaction, and intelligence; Kenneth D Pimple, 'Introduction: The Impacts, Benefits and Hazards of PICT' in Kenneth D Pimple (ed), *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards* (Springer 2014) 2 ('Ambient Intelligence applies particularly to artificial intelligence (AI) devices, but AI capabilities are not excluded by the terms ubiquitous and pervasive').

[237] Information Society and Technology Advisory Group, *Ambient Intelligence: From Vision to Reality* (n 228) 6.

[238] Emilio Serrano and Juan Botia, 'Validating Ambient Intelligence Based Ubiquitous Computing Systems by Means of Artificial Societies' (2013) 222 Information Sciences 3, 3. See also David Wright and others (eds), *Safeguards in a World of Ambient Intelligence*, vol 1 (The International Library of Ethics, Law and Technology, Springer 2008) xxi, who described the research emphasis as being 'on greater user-

'Interactions with people' usually refers to interactions with devices that have significant and uniquely identifiable associations with individuals. Not surprisingly, ISTAG has anticipated the industrial base for ambient intelligence products as arising from consumer electronics companies, car and aeroplane manufacturers, and telecommunications companies, rather than from 'general purpose' computer technology suppliers.[239]

It is clear that the research agendas overlap. However, research agendas attached to the name 'ambient intelligence' are phrased in terms which are human-centred rather than technology-centred. These have a more energetic emphasis on artificial intelligence and context awareness, rather than contrasting ideas of 'everywhereness' implied by the terms ubiquity and pervasiveness. In other words, ambient intelligence definitions tend to focus on the 'ends' rather than the 'means'. This is in contrast to the main area of concentration reflected in the ubiquitous/pervasive computing literature.

However, the emphasis in the ambient intelligence literature on interaction with, and benefits to, human users can obscure some key concerns. In the end, such systems will be built primarily by and for those corporate or government entities with the resources to do so. As a result, the intended beneficiaries of these systems will not necessarily be the individuals who 'use' them: but may instead be companies or governments who wish to monitor their employees' or citizens' movements, or suppliers who want to target advertising of their products to people with a particular data profile. The reliance of ambient intelligence systems on data profiling, being 'the construction or inference of patterns by means of data mining and … the application of the ensuing profiles to people whose data match with them',[240] gives rise to its own specific problems. Hildebrandt and Koops identified four categories of problems generated by profiling:

friendliness, more efficient services support, user empowerment and support to human interactions'.

[239] Information Society and Technology Advisory Group, *Ambient Intelligence: From Vision to Reality* (n 228) 3.

[240] Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 Modern Law Review 428, 431.

1) errors caused by 'incorrect categorisation' (for example, false positives and false negatives);

2) loss of privacy and autonomy;

3) the possibility of unfair discrimination and stigmatisation; and

4) threats to due process.[241]

Other scholars have also expressed concern with the 'rather too sunny view of our technological future' expressed by many people advocating the development of ambient intelligence technologies.[242] In particular, researchers funded by the European Commission spent 18 months in the mid-2000s developing so-called 'dark scenarios' to illustrate potential problems in areas such as privacy, security, identity protection, trust, loss of control, dependency, social exclusion, surveillance and spam.[243] These dark scenarios also help to illustrate a problem with terminology. It is common to talk about individuals 'using' these types of technologies, but, in many cases, it is more accurate to say that the technologies (or their controllers) 'use' the individuals, making them usees rather than users. For example, the technologies are used to gather information about individuals, or to trigger actions based on their movements or preferences. Often, these do not provide any outcome desired by the individual, who may well be acted upon without his or her knowledge.

[241] Ibid 433–88.

[242] Michael Friedewald and others, 'The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues' in John A Clark and others (eds), *Security in Pervasive Computing: SPC 2006* (Lecture Notes in Computer Science vol 3934, Springer 2006) 120. See also Hildebrandt and Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (n 240) 433–88.

[243] See European Commission, Joint Research Centre, Information Society Unit, 'SWAMI Project: Safeguards in a World of Ambient Intelligence' (2005) <http://is.jrc.ec.europa.eu/pages/TFS/SWAMI.html> accessed 14 July 2018; Wright and others (eds), *Safeguards in a World of Ambient Intelligence* (n 238).

In 1998, Philips researchers Zelkha and Epstein first proposed the defining characteristics of ambient intelligence as **embedded**, **personalised**, **adaptive** and **anticipatory**.[244] By 2003, other Philips researchers had added **context-aware** to that list.[245] In contrast, the ISTAG Report in the same year refused to identify any definitional characteristics, as ambient intelligence was to them an 'emerging property',[246] that is, one that had not yet developed clear boundaries. However, by this time research into actual devices had developed to the extent that Aarts and Roovers could attempt to classify existing or potential devices on types of power dependence. These categories were: autonomous devices (for example, self-powered tags, sensors), portables (for example, battery-powered mobile phones) and statics (for example, home servers powered on mains electricity).[247]

In 2009, Cook, Augusto and Jakkula examined the most recent research by industry and academia. As a result, they expanded the definition of the main features of ambient intelligence technologies to include **sensitivity**, **responsiveness**, **adaptiveness**, **transparency**, **ubiquity** and **intelligence**.[248] Another roughly concurrent attempt to define the key characteristics of ambient intelligence produced this list: complexity, a lack of boundaries, unpredictability, heterogeneity, incremental development and deployment and the ability to self-configure and adapt.[249]

---

[244] Zelkha and Epstein, 'From Devices to "Ambient Intelligence": The Transformation of Consumer Electronics' (n 227).

[245] E Aarts and R Roovers, 'IC Design Challenges for Ambient Intelligence' *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition 2003* (IEEE Computer Society 2003) 2, 2. Aarts and Roovers used the term 'contextual awareness', but 'context-aware' has become much more common since this time.

[246] Information Society and Technology Advisory Group, *Ambient Intelligence: From Vision to Reality* (n 228) 3.

[247] Aarts and Roovers, 'IC Design Challenges for Ambient Intelligence' (n 245) 3.

[248] Cook, Augusto and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (n 203) 278–79.

[249] Wright and others (eds), *Safeguards in a World of Ambient Intelligence* (n 238).

3.4 Internet of Things

In spring 1998, at a similar time to the emergence of 'ambient intelligence', Kevin Ashton presented to the multinational consumer goods corporate group, Procter & Gamble, an idea that the addition of RFID[250] and other sensor technologies to everyday objects could create an 'Internet of Things'.[251] The concept of an Internet of Things (also known as '**IoT**') has emerged as part of a model of the future direction for the Internet, in particular as a way to frame current developments in infrastructure and information management.

When the initial literature review for this dissertation was undertaken in 2013–14, the 'Internet of Things' was a widely accepted term in Europe and China. It was less widely used in the US, where other terms such as 'smart object' were preferred.[252] However, the rapid increase in the popularity of the term is one of the most significant changes seen by the author of this dissertation since the commencement of doctoral study in 2013.

Despite its popularity, the definition of the Internet of Things in 2018 is the subject of debate, and there is still no generally accepted definition nor taxonomy.[253] By March 2015, Noto La Diega had counted at least 64 definitional attempts, but found none of them 'entirely convincing'.[254] In 2008, the US National Intelligence Council used the definition:

[250] Radio-frequency identification.

[251] Kevin Ashton, 'That "Internet of Things" Thing' (*RFID Journal,* 22 June 2009) <www.rfidjournal.com/articles/view?4986> accessed 26 February 2015.

[252] Rob van Kranenburg and others, 'The Internet of Things' (1st Berlin Symposium on Internet and Society, 25–27 October 2011) 4.

[253] Guido Noto La Diega, 'Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom' (2016) 9 Journal of Law and Economic Regulation 69, 71; Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56) 11.

[254] Noto La Diega, 'Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom' (n 253) 71 fn 11.

> the general idea of things, especially everyday objects, that are readable, recognizable, locatable, addressable, and controllable via the Internet – whether via RFID, wireless LAN, wide-area network, or other means …[255]

However, the use of the word 'Internet' in this and other definitions incorporates a common misunderstanding. The technical definition of the 'Internet' actually refers to a combination of computer networks using a particular set of communications protocols, most importantly the TCP/IP[256] protocols.[257] Many devices represented as examples of IoT, particularly those which communicate over very short distances, do not need (and often do not use) TCP/IP. For example, electronic door key applications, which lock and unlock doors in response to taps on a smartphone icon, may well communicate with the phone using simpler protocols over Bluetooth or infra-red channels.[258]

In 2014, the International Standards Organisation (**ISO**) and the International Electrotechnical Commission (**IEC**) proposed the following definition of 'Internet of Things', that was less dependent on the Internet internetwork:

> [a]n infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react…'[259]

[255] National Intelligence Council, *Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests out to 2025* (Conference Report, CR 2008–07, April 2008), Appendix F-1.

[256] Transmission Control Protocol and Internet Protocol.

[257] Clarke, 'Origins and Nature of the Internet in Australia' (n 5).

[258] For example, August Smart Lock. See Bonnie Cha, 'A Beginner's Guide to Understanding the Internet of Things' (*recode,* 15 January 2015) <http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/> accessed 3 May 2016.

[259] ISO/IEC JTC 1, *Internet of Things (IoT): Preliminary Report 2014* (ISO 2015) 3.

However, even the ISO and IEC recognised that such a short definition could not capture all of the complexities of the technology.[260]

One common element among the various visions of an Internet of Things is the concept of a mass-scale networking infrastructure that supports 'interdevice internetworking'.[261] This concept envisages the 'tagging' of physical objects with a unique identifier (for example, an electronic product code or EPC).[262] The tags can then be accessed (using automated identification and data collection technologies),[263] and information about the object retrieved elsewhere via one or more networks or internetworking arrangements. This includes information such as what category of object it is, who owns it, where it is physically, where it is in network space, where it has been and where it is going.[264]

Tagging of objects that are then scanned and tracked is not a recently emerged functional concept. For example, as early as January 2005, the American multinational retail corporation, Wal-Mart, was requiring suppliers to apply RFID tags to its shipments.[265] However, what appears to be new about the Internet of Things is that it envisages that far more objects will have chips with communication capabilities embedded, to allow information relating to and/or collected by the physical object to be accessible via the Internet or a private network. This brings with it a

[260] Ibid.

[261] Gershenfeld, Krikorian and Cohen, 'The Internet of Things' (n 22) 78.

[262] EPCglobal Inc, 'EPCglobal' <www.gs1.org/standards/epc-rfid> accessed 14 October 2018.

[263] Like RFID, Near Field Communication and other sensor technologies: Stephan Haller, Stamatis Karnouskos and Christoph Schroth, 'The Internet of Things in an Enterprise Context' in John Domingue, Dieter Fensel and Paolo Traverso (eds), *Future Internet: FIS 2008* (Lecture Notes in Computer Science vol 5468, Springer 2009) 15.

[264] Rolf H Weber and Romana Weber, *Internet of Things: Legal Perspectives* (Springer 2010) 17.

[265] Ian Poole, 'RFID History' (*Radio-Electronics.com*) <www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/development-history.php> accessed 20 February 2015. See also Mark Roberti, 'The History of RFID Technology' (*RFID Journal*, 16 January 2005) <www.rfidjournal.com/articles/view?1338/> accessed 26 February 2015.

perceived need for a greater number of unique addresses available for connected devices (and their processes). This need is one of the factors used by advocates[266] to encourage the deployment of IPv6, a network protocol dealing with address and control information that greatly expands the number of unique addresses available.[267]

Most of the existing installations of RFID and similar technologies are still communicating only within one enterprise or just with a limited number of partner enterprises. This is not really an Internet of Things, but rather an Intranet or Extranet of Things.[268] Even within consumer applications of the Internet of Things, most information is still not disseminated outside its capturing application,[269] at least not for the consumer's benefit. However, note that this technical limitation does not represent protection for consumer data. Many consumer devices have web-based applications associated with them. The supplier of the device commonly collects and disseminates data from these applications for marketing and profiling purposes,[270] and the monetisation of this data forms a significant part of their revenue from the devices.

So, this leads to the question of how the Internet of Things fits in with concepts such as ubiquitous/pervasive computing and ambient intelligence.

---

[266] Kelly Fiveash, 'DeSENSORtised: Why the "Internet of Things" will FAIL without IPv6' (*The Register*, 14 April 2014) <www.theregister.co.uk/2014/04/24/ipv6_iot/> accessed 23 October 2018.

[267] Haller, Karnouskos and Schroth, 'The Internet of Things in an Enterprise Context' (n 263) 21, who estimate that IPv6 could accommodate 2^{128} things.

[268] Dieter Uckelmann, Mark Harrison and Florian Michahelles, 'An Architectural Approach towards the Future Internet of Things' in Dieter Uckelmann, Mark Harrison and Florian Michahelles (eds), *Architecting the Internet of Things* (Springer 2011) 3.

[269] Sarah Rotman Epps, 'There Is No Internet of Things' (*Forbes*, 17 October 2013) <www.forbes.com/sites/forrester/2013/10/17/there-is-no-internet-of-things/> accessed 5 February 2018.

[270] For example, Fitbit's Australian privacy policy as at 30 December 2014 stated, 'De-identified data that does not identify you may be used to inform the health community about trends; for marketing and promotional use; or for sale to interested audiences': 'Fitbit Privacy Policy' <www.fitbit.com/au/legal/privacy-policy> accessed 30 December 2014.

Some commentators consider them as equivalent terms.[271] However, others have a more limited view of the Internet of Things. Chaouchi described the Internet of Things as 'one step further on the path to ubiquitous computing'.[272] More specifically, Weber and Weber have envisioned the Internet of Things as playing a significant role as a 'backbone' or support infrastructure for these other forms of computing. In their view, a fully developed Internet of Things has the capacity to 'enabl[e] smart environments to recognize and identify objects, and retrieve information from the Internet to facilitate their adaptive functionality'.[273] This statement is still somewhat too general to be fully accurate. In order to provide an appropriate support structure, such a backbone should be able to capture and perhaps even consolidate many sources of data-feeds, which could be fed over the Internet to information systems. These information systems could process the data in order to generate finely calibrated commands and pass them back over the network to widely dispersed actuators.

Other envisioned usages, incorporating an increased use of sensor and actuator technologies, include:

> cars warning other cars of traffic jams, a cell phone reminding a person when it was last left next to the keys, a waste-bin inquiring its contents about their recyclability, or a medicine cabinet checking the storage life of the medications in it.[274]

The similarity of these scenarios to ubiquitous/pervasive computing and ambient intelligence scenarios is easy to see. It is not surprising that some commentators have attempted to conflate the idea of the Internet of Things

[271] For example, 'Other terms for the Internet of Things include Internet-connected devices, smart connected devices, wireless sensor networks, machines and devices communicating wirelessly, *ubiquitous computing*, *ambient intelligence*, and smart matter' (emphasis added): Melanie Swan, 'Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0' (2012) 1 Journal of Sensor and Actuator Networks 217, 218.

[272] Hakima Chaouchi (ed), *The Internet of Things: Connecting Objects to the Web* (John Wiley & Sons 2010), xi.

[273] Weber and Weber, *Internet of Things: Legal Perspectives* (n 264) 1.

[274] Ibid 1–2.

and the other forms of computing discussed above. For example, Santucci, presenting to the International Conference on Future Trends on the Internet, said 'over the years Europe "forgot" the term "Ambient Intelligence", which it had invented, and "imported" and re-used the term "Internet of Things"'.[275]

However, the majority of the scholarly technical literature (as opposed to popular literature) indicates that the definition of the Internet of Things is not 'the same' as ambient intelligence or ubiquitous/pervasive computing. The Internet of Things is more accurately explained as a subset to these concepts, or as part of a technological path towards their implementation.[276] In 2015, the author of this dissertation was of the opinion that 'considering the history of the other terms and their convergence, it is not impossible that in time the increasing popularity of the term, especially in Europe and in China, may subsume the other definitions and incorporate their characteristics'.[277] At that time, it was certainly the most popular of the terms in the public mind, and that dominance has continued and significantly strengthened over the ensuing three years. **Figure 2** and **Figure 3** below show the results of two searches run on Google Trends (for 2005–14 and 2014–18 respectively) that indicated the trends in the frequency with which the terms 'ambient intelligence', 'ubiquitous computing', 'pervasive computing', and 'Internet of Things' had been searched for using a leading search engine.

[275] Gerald Santucci, 'From Internet of Data to Internet of Things' (International Conference on Future Trends of the Internet, Luxembourg, 28 January 2009) 2–3.

[276] Weber and Weber, *Internet of Things: Legal Perspectives* (n 264) 1; Chaouchi (ed), *The Internet of Things: Connecting Objects to the Web* (n 272) Preface.

[277] Manwaring and Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (n 84) 59.

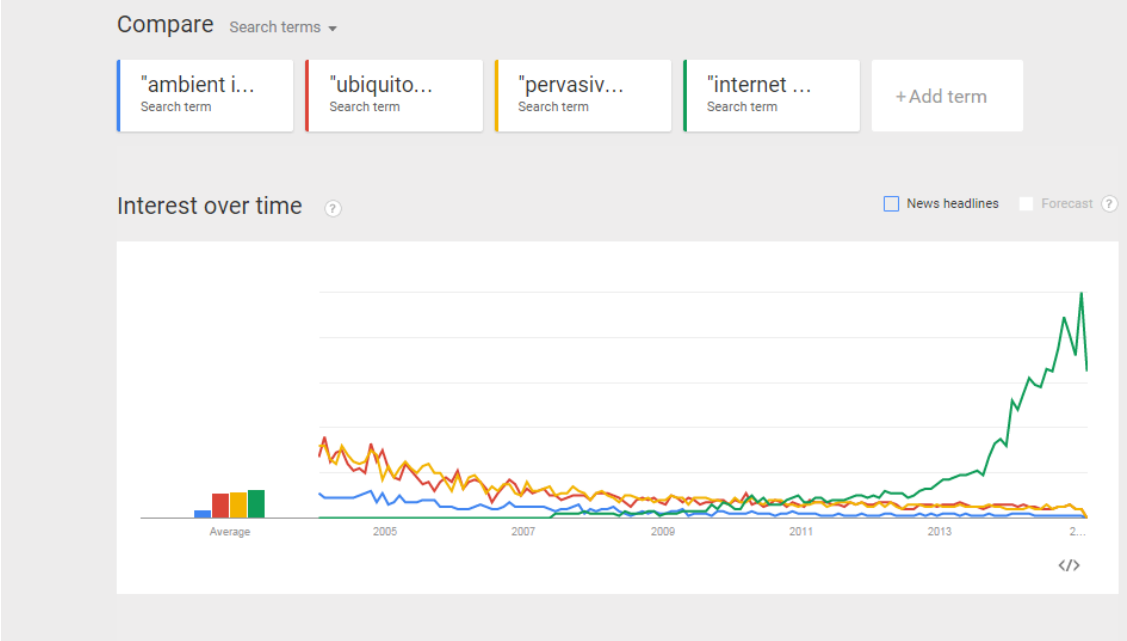

Figure 2: Popularity of search terms 'ambient intelligence', 'ubiquitous computing', 'pervasive computing', 'Internet of Things' (1 Jan 2005 to 1 Dec 2014).[278]

[278] Data Source: Google Trends (www.google.com/trends). In terms of *content* from all sources, a Google search run by the author of this dissertation on 1 December 2014 gave the following results: 'Internet of Things', about 15 800 000; 'ubiquitous computing' 689 000; 'pervasive computing' 651 000; 'ambient intelligence' 438 000. However, a search on Google Scholar reveals that at least this subset of the academic literature reflects roughly opposite proportions.

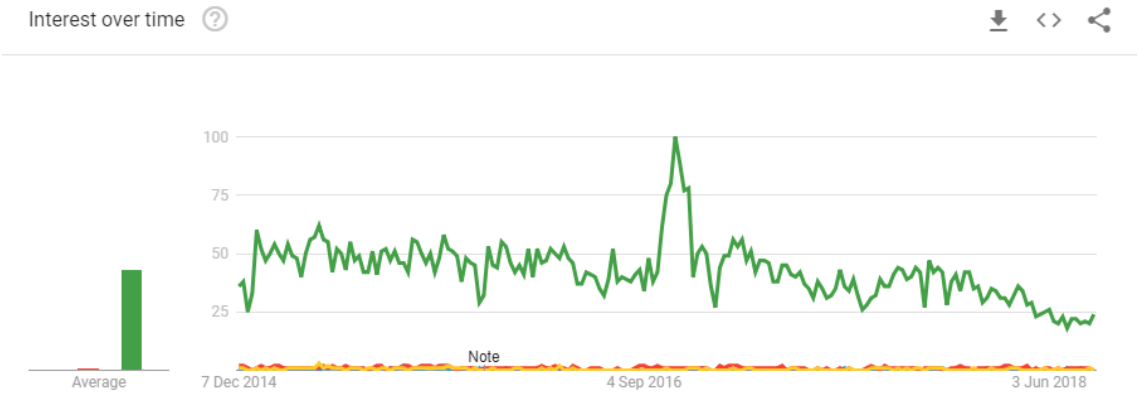

Figure 3: Popularity of search terms 'ambient intelligence', 'ubiquitous computing', 'pervasive computing', 'Internet of Things' (2 Dec 2014 to 20 Aug 2018)[279]

However, since 2015 to the present time, no real clarity or consensus has emerged around a definition of the 'Internet of Things', despite the term's increase in popularity. Attempts at definitional clarity have predominantly (although not entirely[280]) been abandoned, particularly as technological, policy and legal research study is tending to fragment into more granular technology types or subsets of the technology.

When considering the technical (as opposed to popular) definitions, a major limiting factor is the insistence on a global communications and information-sharing network as an essential requirement. For example, Uckelmann, Harrison and Michahelles consider that the Internet of Things can currently be differentiated from ubiquitous/pervasive computing because the latter 'does not imply the usage of objects nor does it require a

[279] Data Source: Google Trends (www.google.com/trends). In terms of *content* from all sources, a Google search run on 20 August 2018 gave the following results: 'Internet of Things', about 42 000 000; 'ubiquitous computing' 1 730 000; 'pervasive computing' 1 500 000; 'ambient intelligence' 573 000. The Google Scholar results still reflected the opposite: 'Internet of Things' 185 000; 'ubiquitous computing' 291 000; 'pervasive computing' 249 000; 'ambient intelligence' 59 900.

[280] One notable exception is Jatinder Singh and others, 'Accountability in the IoT: Systems, Law, and Ways Forward' (2018) 51 Computer 54.

global Internet infrastructure.'[281] This distinction could apply equally well to ambient intelligence. For example, the ambient intelligence scenario of clothes made of smart materials that sense perspiration and adjust ventilation[282] does not require a connection to the Internet. Both ubiquitous/pervasive computing and ambient intelligence, as definitional terms, envisage a localised, globalised, (and potentially a universal), implementation: the 'Internet of Things', at least in its present manifestation, is more confined. Localised silos of connected things do currently exist[283] and are likely to exist in the future. However, as discussed above they should preferably be distinguished from the Internet of Things by using terms such as 'intranet of things'.[284] It is also important to note that many localised systems will not run TCP/IP protocols, but some form of alternative protocol due to the limited resources or 'volatility' of devices on the periphery, as discussed in **section 4.2.4** of this chapter.

3.5 Towards a framework

While this chapter has identified some differences between the common terminologies, it cannot be said that any of these forms of computing have clear-cut boundaries separating them. It appears rather that mobile computing and the Internet of Things are best characterised as subsets of a broader type of computing, involving technological paths to achieving visions of ubiquitous computing or ambient intelligence. Discussions in the literature of broader visions of ubiquitous/pervasive computing and ambient

[281] Uckelmann, Harrison and Michahelles, 'An Architectural Approach Towards the Future Internet of Things' (n 268) 5. These authors do not expressly consider the possibility of a localised 'Internet of Things'. See also Tomas Sanchez Lopez, 'What the Internet of Things is NOT' (*Technical Blog,* 22 March 2010) <http://technicaltoplus.blogspot.com.au/2010/03/what-internet-of-things-is-not.html> accessed 1 June 2017.

[282] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 426. Note that this scenario is provided in a book that is ostensibly about ubiquitous computing, not ambient intelligence.

[283] Singh and others, 'Accountability in the IoT: Systems, Law, and Ways Forward' (n 280) 54.

[284] Michele Zorzi and others, 'From Today's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View' (2010) 17 Wireless Communications, IEEE 44.

intelligence do not usefully assist in identifying differences, as they routinely throw up similar forms of technology, just viewed through different dominant functional lenses: such as an emphasis on 'everywhereness' for ubiquitous/pervasive computing, and 'adaptability to humanness' for ambient intelligence. However, a map of the functional lenses creates a simplified but useful starting point. **Figure 4** presents such a map, summarising the relationship among the terms based on these functional lenses.

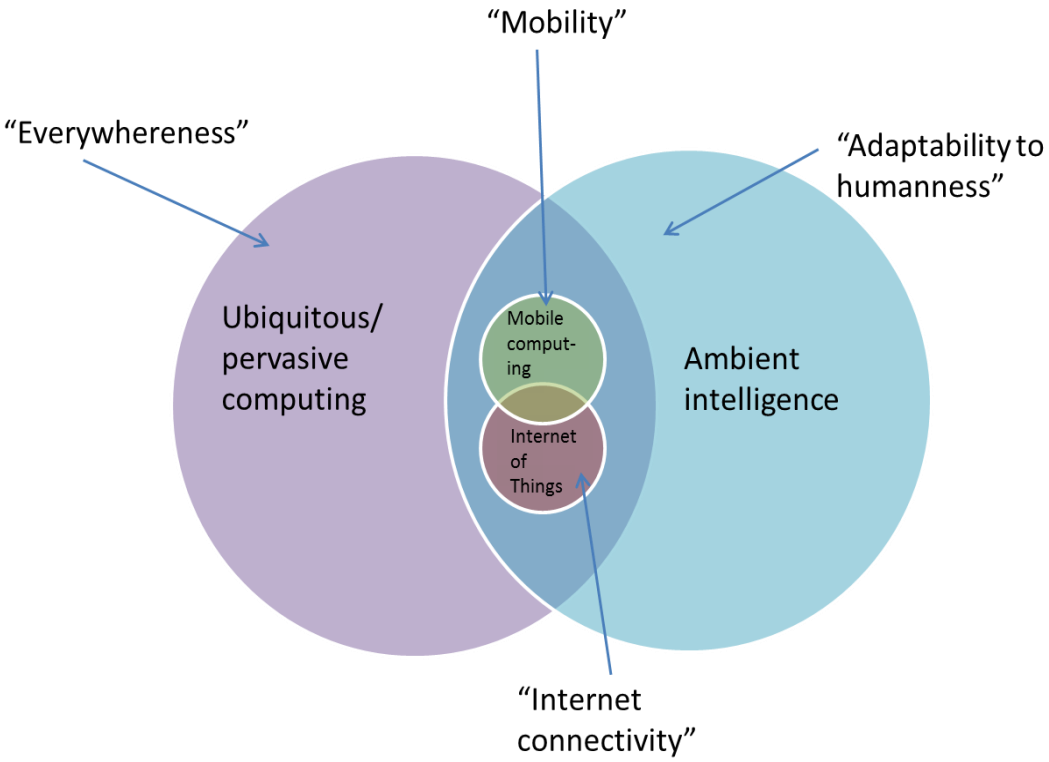

Figure 4: Dominant functional lenses of ubiquitous/pervasive computing, ambient intelligence, mobility and Internet of Things

However, simple diagrams and express definitions are open to challenge, as they cannot accurately reflect the complexity of the new model, or inconsistencies within the literature. The model is better described through a framework that deals with key attributes, both technical and functional.

4 TECHNICAL RESEARCH FRAMEWORK

4.1 Construction: key attributes in the literature

As set out in **section 3** of this chapter, scholars have made various attempts to describe the dimensions of this new form of computing. This chapter distinguishes possible characterisations of technology within the new model in order to assist in understanding their impacts. In particular, it assists in predicting where challenges might arise for existing regulatory frameworks. The framework is intended to provide guidance when researchers want to evaluate how existing or proposed legal, economic and/or policy models will work when confronted with the sociotechnical change brought about by these technologies.

An initial identification of the key dimensions of this new model of computing makes sense as a first step in this analysis. A subsequent chapter will take the next step of identifying how these characteristics, by themselves or in combination, differ from existing technologies in ways that might give rise to unique legal problems.

Before the first steps are taken, it is sensible to consider what term might be used to refer to the new model. The concept of 'third wave' computing, although tenable, is somewhat too general to be fully useful. As the previous section has shown, no one of the major terms discussed is satisfactory. As an alternative, this dissertation adopts the term 'eObject', to refer not to the model as a whole, but rather to the central element underlying the new model. The concept of 'object' is general enough to include both natural things and artefacts, and encompasses living things such as humans and animals. The use of the 'e' follows a tradition set by existing terms such as 'e-commerce.' However, its use here is intended to reflect a broader concept than that of electronic computing or use of the Internet. It describes objects as diverse as phones, walls, buildings, trees, animals and people that are enhanced through the embedment of computing power and communications capabilities.

Previous attempts to identify the characteristics of the variants of eObjects have tended to concentrate on two dimensions: core functional attributes and types of devices or systems. From the existing literature, the most commonly mentioned attributes of eObjects can be summarised as:

- increased device portability;[285]
- increased use of remote telecommunication services;[286]
- embedment of data handling capabilities in objects or in environments not previously computerised;[287] and
- increased use of internetworking by devices which are partially or wholly autonomous from human users.[288]

Other important attributes of eObject devices and systems that also appear in the literature include:

- devices and systems that are designed to be invisible or unobtrusive to humans;[289]
- devices capable of communication that are intended to populate all/many places, or to provide comprehensive coverage of a specific location;[290]

[285] For example, Mahadev Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (1996) *Principles of Distributed Computing: Proceedings of the Fifteenth Annual ACM Symposium* 1, 1.

[286] For example, Weiser, 'The Computer for the 21st Century' (n 19) 101–02; Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 19.

[287] For example, Ashton, 'That "Internet of Things" Thing' (n 251); National Intelligence Council, *Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests out to 2025* (n 255) app F1–F2.

[288] For example, Pimple, 'Introduction: The Impacts, Benefits and Hazards of PICT' (n 236) 2; Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 9.

[289] For example, Weiser, 'The Computer for the 21st Century' (n 19) 94; Singh, Puradkar and Lee, 'Ubiquitous Computing: Connecting Pervasive Computing through Semantic Web' (n 191) 422.

[290] For example, Weiser, 'The Computer for the 21st Century' (n 19); Lyytinen and Yoo, 'Issues and Challenges in Ubiquitous Computing' (n 185) 63–64.

- humans interacting with many devices;[291]
- devices interacting with many other devices, over internetworks, often without human intervention;[292]
- mobility of the device and/or the human: therefore devices can be mobile, tethered or anywhere in-between;[293]
- devices and/or their interactions can be personalised to their human users;[294]
- devices are often volatile, in relation to their connections to the Internet and other internetworks, their resources and processing speed;[295]
- devices and systems are often more vulnerable to security issues than other types of information and communication technologies, due to both physical and technical design features;[296]
- devices are context-aware;[297]
- objects are capable of being uniquely identified;[298]

[291] For example, Weiser and Brown, 'The Coming Age of Calm Technology' (n 6) 78.

[292] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 9.

[293] For example, Lyytinen and Yoo, 'Issues and Challenges in Ubiquitous Computing' (n 185) 64.

[294] For example, Zelkha and Epstein, 'From Devices to "Ambient Intelligence": The Transformation of Consumer Electronics' (n 227).

[295] For example, Satyanarayanan, 'Pervasive Computing: Vision and Challenges' (n 190) 11, 13–14; Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (n 285) 1; Coulouris and others, *Distributed Systems: Concepts and Design* (n 192) 817.

[296] For example, small portable devices such as fitness trackers and mobile phones are more susceptible to physical theft or damage: Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (n 285) 1. There is also some evidence emerging that many eObjects are inherently more vulnerable to security breaches: Cook, Augusto and Jakkula, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (n 203) 286–87.

[297] For example, Aarts and Roovers, 'IC Design Challenges for Ambient Intelligence' (n 245) 2.

[298] For example, Haller, Karnouskos and Schroth, 'The Internet of Things in an Enterprise Context' (n 263) 15.

- objects are locatable in network space and in real space (geo-locatable);[299] and
- devices often have a significant dependence on external infrastructure, such as satellites or location APIs[300] (for location-tracking) and physical sites into which devices are integrated (such as bathroom shelves and bus shelters).[301]

4.2 The framework

4.2.1 A working definition and some of its limitations

The following working definition is adopted:

> An eObject is an object that is not inherently computerised, but into which has been embedded one or more computer processors with data collection, data handling and data communication capabilities

Due to the complexity of the model, however, this working definition does not give a complete view of the technologies encompassed within the third wave of computing. It must also be noted that this particular working definition is likely to have a limited shelf life, due to the use of the words 'not inherently computerised'. It is easy to imagine a world, in the medium- to long-term at least, where a concept of what is and is not 'inherently computerised' has changed dramatically.

The difficulties this raises can be seen most clearly in relation to one of the key technologies discussed in this chapter, the mobile phone, or smartphone.[302] The 'tab', a smartphone-like device, was one of the early ideas pursued by Weiser and Xerox PARC in their development of ubiquitous

[299] National Intelligence Council, *Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests out to 2025* (n 255) Appendix F-4.

[300] Application Program Interfaces.

[301] For example, Gershenfeld, Krikorian and Cohen, 'The Internet of Things' (n 22) 78.

[302] The difficulty of applying this definition to smartphones was raised by an anonymous reviewer of Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

computing. Original telephones were not inherently computerised. However, while the exact definition of a smartphone itself is contentious,[303] the need for some form of computerisation is not at issue in that contention. It will not be long before a computer processor will be embedded in *all* phones (other than those kept as historical artefacts).

For the purposes of this dissertation, smartphones are included in the definition of eObject, as they contain all of the **core attributes** listed in **section 4.2.2** of this chapter. Some definitions of the 'Internet of Things' exclude smartphones, tablets and other like devices specifically from their definition.[304] Such devices constitute notably a *transitional* technology and therefore create some definitional dissonance between 'conventional' and 'new' forms of computing. However, when considering the sociotechnical landscape of the third wave (and indeed even within the narrower concept of 'Internet of Things'), the role of smartphones and tablets cannot be ignored. These devices and the applications installed on them form an integral part of many systems in which other eObjects participate, primarily as a remote controller and also often the device to which data is transmitted and delivered to humans in an intelligible form.[305]

The scope of third wave technologies is much more complex than can be fully encapsulated in a shorthand definition. Therefore, in order to assist in a more detailed understanding of the technological landscape, this dissertation formulates a framework with 3 key dimensions: **core attributes** of the technology, the **interactions** among devices, systems and living things, and **other attributes** (attributes commonly but not always found in eObjects). While the current short working definition adopted in this dissertation may have a comparatively short life before needing refinement, the attributes and

[303] Andrew Charlesworth, 'The Ascent of Smartphone' (2009) 4 Engineering and Technology 32, 32–33.

[304] Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (n 67) 5; Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56) 458.

[305] Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (n 67) 5; Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56) 458.

interactions are defined at a sufficient level of generality so that they should still be applicable in the long term. There may also be other attributes or interactions that emerge over time.

4.2.2 Core attributes

The core attributes of an eObject are elaborated in **Table 2**. These attributes are intended to be definitional: that is, a devices or system that is missing one or more of them is not considered an 'eObject'.

Table 2: An eObject's core attributes

Attribute	Description
Object	Is a physical object, which may be natural or an artefact, of any size, and inert or living
Computer	Contains one or more general-purpose programmable computers, sufficiently miniaturised
Embedded	One or more computers are physically embedded in the object (as distinct from being socially, culturally or metaphorically embedded)
Data collection	Contains one or more sensors that can collect or generate data. Note that sensors are a core attribute, while actuators are not: an ability to act in a physical manner on the environment is common in eObjects, but not essential (other than the ability to communicate data)
Data handling	Can process data
Data communication	Can communicate with other nodes inside the same object, or with other objects[306]

eObjects are often not stand-alone objects, but may be nested within a larger object, or may be used as elements of a larger, probably distributed system.

[306] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 426 postulates the development of 'clothes [that] could sense human skin and reconfigure itself to offer more ventilation if it senses the skin is sweating'.

Many physical objects are combinations of other objects, and some or all of these combined objects can be eObjects. For example, a smart refrigerator may contain a number of eObjects including: shelves which contain sensors to track products coming in and out via barcodes or RFID tags; an LCD screen with the capability to display notes and order new goods via the internet; and a door and walls containing sensors and actuators which track light, room temperature and door opening frequencies and adjust cooling temperature accordingly.[307]

The entity arising from this combination or 'nesting' of eObjects is not limited to physical objects such as home appliances. Systems may be made up of a number of eObjects interacting with each other, living things and/or the physical world, even though the system itself may not be an eObject within the definition above. For example, a home automation system may use:

- embedded processors in its air conditioning, lights, locks, curtains and power supply;
- the owner's smartphone and its applications; and
- a security company's computing and communications devices.

4.2.3 Interactions

Interactions among the various types of eObjects and systems represent the second key dimension within the framework. eObjects can interact with living things, the physical world, each other, and other computing devices and systems. These interactions can be technical, physical or social. The distinction between interaction types is important to consider when researching the efficacy of existing regulatory frameworks, as the types of interactions may affect relationships between consumers, businesses and governments involved with the technologies. Also, particular types of interactions may raise policy expectations that are different depending on the interaction. For example, citizens may well expect stricter forms of

[307] See for example, George Wilkenfeld, 'Smart Meters, Displays and Appliances' (*Australian Government*, 2013) <www.yourhome.gov.au/energy/smart-meters-displays-and-appliances> accessed 20 August 2018.

regulation on an eObject acting on a living thing, as opposed to something that merely interacts with other computing devices and systems. Some examples of interactions relevant to legal, economic and policy research include:

a) Interactions with living things
   eObjects may have a number of different types of interactions with living things. For example, an eObject may accept input from, or measure something about, a person, animal or plant. If it contains an actuator, it may also act upon that living entity in a physical way. A simple example is a Fitbit fitness device which counts steps taken, and then vibrates to let the user know when a target goal has been achieved.[308] At the other end of the scale of complexity is cyborgisation, where legal and policy problems have already been identified, particularly where the implantation that transforms a person into an eObject is involuntary.[309]

b) Interactions with other eObjects or systems
   eObjects may have interactions with other eObjects or systems which are permanent, or temporary. Many of the eObjects in a smart home will have permanent interactions among them, as they are in fixed locations and are initially designed to work together. A temporary interaction might occur where the processing or communication capabilities of an eObject are co-opted by a system into whose proximity the eObject has been brought. For example, iBeacon devices installed in shops are designed to communicate with passing mobile phones, and mobile phone applications 'listening' for relevant iBeacon signals can trigger notifications of discounts or requests for payment on the phone.[310] This

[308] Fitbit <www.fitbit.com/au/home> accessed 23 August 2018.

[309] Clarke, 'Cyborg Rights' (n 152).

[310] Pointr, 'Beacons: Everything You Need to Know' <www.pointrlabs.com/posts/beacons-everything-you-need-to-know/> accessed 5 September 2018.

interaction may lead to the creation of a contractual relationship and/or a duty of care.

4.2.4 Other attributes

The third of the key dimensions in the framework is concerned with eObjects' other attributes, which are presented in **Table 3** (in alphabetical order, not in any order of precedence). Even though they fall outside of the core definition, they are included within the framework because their existence, inter-relationships, and even the frequency with which they appear can help define various sub-sets within the eObject model. In addition, examination of these other attributes can lead to more specific and detailed analysis of problems that might arise in relation to an eObject. For example, those interested in researching the protection of location information (from either a legal or strategic business perspective) would be particularly interested in objects or systems that are **vulnerable**, **identifiable** and **geo-locatable**.

Table 3: eObjects' other attributes (in alphabetical order)

Attributes	Limits
Active capacity	An eObject may be able to perform acts which have an impact on the physical world, through the use of different types of actuators (devices which move things).
Adaptability	An eObject may adapt or be responsive to context (eg, physical environment) and/or an individual (often referred to as 'context-awareness').
Addressability	An eObject may have, at any given moment, an address that is unique, and that is at least potentially knowable (eg, IP address, cell address, geo-coordinates).
Associability with living beings	An eObject may have degrees of personal association (either physical, emotional or based on a legal relationship) with particular individual humans and/or groups. These can range from family cars, to phones, to jewellery, to chips implanted in the human body. Associations may also exist with animals or plants (eg, tracking movement or propagation of endangered populations).

Attributes	Limits
Autonomy	An eObject may be fully autonomous or have some degree of autonomy from human users or systems of which they form a part. The decision-making capabilities of eObjects may exhibit varying degrees of sophistication.[311]
Dependency	An eObject may depend on services and/or infrastructure located outside of the eObject itself.
Geo-locatability	Any particular eObject, or all eObjects in a system, may be locatable in universal physical space or some bounded physical space.
Identifiability	An eObject may have one or more identifiers each of which may be unique, and each of which may be at least potentially knowable (eg, an EPC for a physical object, International Mobile Equipment Identity (IMEI) number for mobile phone handsets, International Mobile Subscriber Identity (IMSI) number for GSM SIM cards, Media Access Control (MAC) address for a network interface card).
Mobility	An eObject may be operational while moving within a physical space, when used by a person on the move or acting autonomously. A system that has eObjects as elements may maintain services to people while they are on the move, or conduct autonomous operations, within some bounded physical space, by utilising services provided by multiple eObjects or successive eObjects encountered by any of its elements while on the move.[312]

[311] Many authors have classified the decision-making aspects of this attribute as an 'intelligent' response. The term 'intelligent' has not been used for the reasons discussed in **section 3.2.1** of this chapter and n 233.

[312] Mobility and portability are often conflated in the literature. However, some authors have acknowledged the difference between the two concepts while still using the umbrella term 'mobility': see for example, Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (n 144) 34. To better acknowledge the difference between the two concepts, two different terms have been used.

Attributes	Limits
Network locatability	Any particular eObject, or all eObjects in a system, may be locatable in universal network space or some bounded network space.[313]
Operational, economic and social impact	An eObject's features and performance may be beneficial to some parties and detrimental to others.
Portability	An eObject may be fixed in place, somewhat limited in movement by cables and connectors (ie, tethered) or fully portable. Note that this is a subtly different concept from that of mobility: a mobile eObject operates while on the move, whereas one which is merely portable can move from one physical place to another, but does not operate while in transit.[314]
Prevalence	A category of eObjects, or a system that uses eObjects to perform some function, may be in many places ('pervasive'), or in all places ('ubiquitous').
Use pattern	An eObject or multiple eObjects may be used with various frequencies, including only once, spasmodically, regularly, continually, or continuously.
Visibility	An eObject may be clearly visible to a person as a computerised data collector, processor and communicator or have different levels of visibility to the point that the eObject interface is unobtrusive or invisible. The object itself may be large or obtrusive, but its nature as an eObject may be unobtrusive or invisible. Interaction with the eObject may involve different levels of explicit, implicit or no human computer interaction.
Volatility	Due to its design features, an eObject may have variable connectivity, restricted energy, limited storage capacity and slow or intermittent processing capabilities.

[313] Although note that 'devices can appear and disappear on the network intermittently, either to save energy or because they are on the move': Neil Gershenfeld and JP Vasseur, 'As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things' (2014) 93 Foreign Affairs 60, 65–66.

[314] See n 312.

Attributes	Limits
Vulnerability	An eObject may be more or less vulnerable to security breaches, theft, and physical damage or destruction.

In the 2015 article on which this chapter is based, the attribute of 'Visibility' was referred to as 'HCI', the abbreviation for 'human-computer interaction'.[315] However, on further consideration, 'visibility' emerged as a better term. It is broader, encapsulating devices on a spectrum of visibility, but which have no level of human-computer interaction. For example, eObjects that are not associated with a person may have very low levels of visibility in terms of their 'enhanced' nature, but nevertheless collect, process and communicate data on persons, such as shop-entrance sensors, advertising boards, drones and rubbish bins.

5 CONCLUDING REMARKS

This chapter has examined the current literature on the 'third wave of computing', in order to better define and understand it for the purposes of conducting research. This dissertation uses the technical research framework developed in this chapter to examine the impact the third wave may have on existing legal rules and frameworks. The development of this framework was necessary because the existing literature, not surprisingly for an area of significant innovation, did not contain a clear description of this 'third wave', but rather a number of terminologies and definitions that are evolving, overlapping and inconsistent.

The chapter has proposed the notion of an 'eObject'. The core properties of an eObject consist of the embedment in objects of computers with data collection, data handling and data communications capabilities. These eObjects may be stand-alone, or may be nested within a larger object, or comprise an element or elements of a larger, distributed system. Further, the

[315] Manwaring, 'Surfing the Third Wave of Computing: Contracting with eObjects' (n 3) 151.

chapter recognises that there are many other properties of relevance to these types of technologies, and a variety of interactions among them.

The identification of core and other properties provides a depth of appreciation of the nature of eObjects. Much legal scholarship in the area has lacked a comprehensive and consistent view of the technology under discussion. A clearer understanding of the technologies involved was necessary in order to properly explore its implications, and its potential impact on consumers. This chapter has proposed a framework within which this dissertation is able to analyse the features in depth, with a particular focus on the examination of legal problems that might arise from particular aspects of sociotechnical change brought about by eObjects.

The next chapter (**Chapter 3**) sets out the conceptual framework used in this dissertation, and an approach to uncovering legal problems in the face of sociotechnical change arising out of eObjects.

Chapter 3 – Legal problems and sociotechnical change[316]

[316] This chapter reproduces significant parts of a research paper published online and a journal article published during the course of doctoral study: Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (n 90); Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

1 AIMS OF CHAPTER

> In th[e]... context of rapid technological change, the contours of legal and regulatory action are not obvious, nor are the frames for analysis.[317]

The study of law and technology and the closely related, but broader, study of regulation and technology, are specialisations which are still emerging, and the contours of those research areas are not fixed. This chapter provides an overview of the emerging conceptual foundations and literature in this area. The theoretical literature is still in early stages of development, and therefore contains some limitations. Despite these limitations, the perspectives and approach discussed in this chapter can provide a useful frame of reference for examining sociotechnical change brought about by eObjects, and particularly the legal implications of this change.

The aim of this chapter is to outline and justify the conceptual framework used in this dissertation to identify and examine legal problems associated with eObjects and the systems in which they participate. As Antonenko explains, 'an effective conceptual framework plots the conceptual landscape of the problem and charts possible routes to explore it'.[318] **Section 2** of this chapter presents a map of the conceptual landscape, identifying the location of the enquiry on ten general dimensions of law and technology research. It also identifies and elucidates some of the less understood and more contentious aspects in law and technology research, such as the nature of sociotechnical change and the pitfalls of technological neutrality.

[317] Roger Brownsword, Eloise Scotford and Karen Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 4.

[318] Pavlo D Antonenko, 'The Instrumental Value of Conceptual Frameworks in Educational Technology Research' (2015) 63 Educational Technology Research and Development 53, 67.

Section 3 explores the research approach, or 'route', adopted in this dissertation to explore the landscape of the enquiry. **Section 3** examines the nature of this proposed approach, most importantly the categories of legal problems that can arise in the context of sociotechnical change. It emphasises that not every incidence of sociotechnical change necessarily operates outside the scope of existing legal rules. The section also proposes some modifications to the proposed approach, in order to better fit with the level of the abstraction of the technology examined in this dissertation, as well as the necessary constraints of a doctoral study.

For the reasons given in **section 3** of this chapter, a key part of the conceptual approach adopted requires the identification of the goals and purposes of the existing legal rules that may be relevant to the sociotechnical change at issue. Therefore, this chapter continues on in **section 4** to identify the goals of the Australian laws relating to consumer contracts.

The conceptual framework developed in this chapter is then applied in **Chapters 5**, **6** and **7** of this dissertation to examine the potential legal implications arising out of the sociotechnical change brought about by the attributes and interactions of the technologies discussed in **Chapter 2**.

2 THE DIMENSIONS OF THE RESEARCH

Some doubt has been thrown on the possibility that coherent broader theories of law and technology, or regulation and technology, are possible given the plethora of different technologies that could be included.[319] Despite this doubt, some scholars have begun to sketch out general 'analytic tools [to] help understand what this discipline is about, how it approaches its

[319] Brownsword, Scotford and Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' (n 317) 7; Arthur J Cockfield, 'Towards a Law and Technology Theory' (2004) 30 Manitoba Law Journal 383, 387; Gregory N Mandel, 'Legal Evolution in Response to Technological Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 226; Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 313.

research … [and] … what it can contribute to the body of knowledge'.[320] Commentators have also expressed the hope that conceptual developments in law and technology theory could provide a basis for broader and better-informed doctrinal legal analysis.[321]

This process of 'reflecting back'[322] theory onto practice in the form of doctrinal analysis is not one-way, but rather cyclical and iterative. Doctrinal analysis can provide a practical and informed perspective on the validity of general conceptual approaches to law and technology research. This dissertation, and particularly the deep doctrinal analysis of a particular area of law, is used as a case study to provide insights into the usefulness and applicability of the chosen conceptual framework and approach to law and technology research set out in this chapter. These insights are discussed in **section 2.2** of **Chapter 8**.

As a starting place for research, Koops helpfully suggests that scholars locate themselves along ten dimensions organised into three 'constitutive elements' or 'regions':

1) Technology region: *technology type, innovation, time* and *place*;[323]
2) Regulation region: *regulation type, normative outlook* and *knowledge*;[324] and
3) Research region: *discipline, problem* and *frame*.[325]

Sections 2.1 and **2.2** of this chapter locate the research undertaken for this dissertation along each of these dimensions, and illustrates the conceptual tools that scholars have used to frame law and technology research in each of these regions. This process allows the development of a conceptual

[320] Koops, 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' (n 145) 325.

[321] Cockfield and Pridmore, 'A Synthetic Theory of Law and Technology' (n 23) 496.

[322] Ibid 496.

[323] Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 314–18.

[324] Ibid 318–20.

[325] Ibid 320–22.

framework and approach through which the research can be viewed and conducted. Koops' dimensions are not framed in, nor dependent on, a linear or chronological structure. Therefore, in order to provide a clearer line of argument, this section discusses the dimensions in a different order than does Koops.

2.1 Dimensions discussed in preceding chapters

Some of the more obvious locations of the dimensions of *technology type*, *regulation type*, *discipline*, *normative outlook* and *frame* have already been pinpointed in the preceding chapters, and are briefly summarised in this section.

2.1.1 The *technology type* dimension

As discussed in **section 2** of **Chapter 2**, Koops proposes that questions of regulation raised by individual instances of sociotechnical change 'depend very much on the character and level of the technology at issue', that is, the *technology type*.[326] For example, in terms of the character of a technology, the issues raised by most information and communication technologies (ICT) are likely to be different from those brought about by genetic technologies. With regards to level of abstraction, the questions raised by a very specific technology such as Instagram will vary significantly from those raised by a discussion of 'ICT' as a general area of research.[327]

The *technology type*, including its level of abstraction, discussed in this dissertation was introduced in **Chapter 1** and discussed in detail in **Chapter 2**. A clear exposition of the level of abstraction is particularly important. At a practical level, the required step (discussed at **section 3** of this chapter) of identifying the existing law applicable to a particular kind of sociotechnical change will depend profoundly on the level of abstraction identified. Laws of general application may well apply across different levels of abstraction. However, the process of *identification* of relevant laws cannot

[326] Ibid 312.

[327] Ibid 312–13.

be achieved accurately in the absence of a good understanding of the technology type.

2.1.2 The *regulation type* dimension

Chapter 1 of this dissertation identified the *regulation type* underpinning this enquiry as 'law', that is, 'authoritative rules backed by coercive force, exercised … by a legitimately constituted (democratic) nation-state.'[328] This is not to say that law is the *only* way to attempt to direct consumer and commercial behaviour and outcomes.[329] Rather, legal rules form a subset of a broader concept of 'regulation'. The definition of regulation is contentious and contextual,[330] but in the limited context of this dissertation Black's 2002 wide-ranging but well-used definition of regulation will suffice:

> the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification.[331]

[328] Brownsword, Scotford and Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' (n 317) 6.

[329] Ibid.

[330] See for example the discussion in Karen Yeung, 'Are Human Biomedical Interventions Legitimate Regulatory Policy Instruments?' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 834–35; and Lyria Bennett Moses, 'Regulating in the Face of Sociotechnical Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *Oxford Handbook of Law and Regulation of Technology* (OUP 2017) 575–76.

[331] Julia Black, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1, 26. This definition has been used in a number of subsequent works, for example: Ronald Leenes, 'Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology' (2011) 5 Legisprudence 143, 149; Benoit Dupont, 'Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation As a Way to Control Large-Scale Cybercrime' (2017) 67 Crime, Law and Social Change 97, 103; Colin Gavaghan, 'Lex Machina: Techno-Regulatory Mechanisms and Rules by Design' (2017) 15 Otago Law Review 123, 124; Steven White, 'Standards and Standard-Setting in Companion Animal Protection' (2016) 38 Sydney Law Review 463, 468. Black's definition builds on an earlier definition by Philip Selznick, 'Focusing Organisational Research on Regulation' in R Noll (ed), *Regulatory Policy and the Social Sciences* (California UP 1985) 363–64.

Regulatory problems outside the relatively narrow context of 'law', for example those resulting from attempts to promote organisation or industry self-regulation, *can* arise out of sociotechnical change. However, due to *frame* constraints (discussed in more detail in **section 2.1.4** of this chapter) the location of this enquiry on the *regulation type* dimension is **not** centred in this wider context of regulation. Nor does the dissertation discuss the possibility of law itself acting as a form of 'technology'.[332] Most notably, it does not include a discussion of 'techno-regulation',[333] or technology acting as a form of law or regulation itself, as most famously proposed by Lessig.[334] eObjects and the systems in which they participate almost certainly have the potential to act, or be caused to act, in a regulatory manner,[335] but further examination of this issue is beyond the scope of this dissertation.

2.1.3 The *discipline* dimension

Reflecting the *regulation type* chosen, the approach taken in this dissertation is situated primarily in the academic legal *discipline.* However, as discussed in **Chapter 1**, this dissertation is also constrained by a narrower field of enquiry contained within the broader discipline, that of legal rules relating to consumer contracts.

[332] See for example, Brownsword, Scotford and Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' (n 317) 5.

[333] Roger Brownsword, 'Techno-Regulation, Human Rights and Human Dignity' in Roger Brownsword (ed), *Human Rights* (Hart Publishing 2004). See also Mireille Hildebrandt, 'Algorithmic Regulation and the Rule of Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Engineering Sciences.

[334] Lawrence Lessig, *Code and Other Laws of Cyberspace* (Basic Books 1999). See also: Bronwen Morgan and Karen Yeung, *An introduction to law and regulation: text and materials* (Cambridge University Press 2007) 102-105; Roger Brownsword, 'Code, control, and choice: why East is East and West is West' (2005) 25 Legal Studies 1; Brownsword, 'Techno-Regulation, Human Rights and Human Dignity' (n 333).

[335] See for example, Hildebrandt and Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (n 240) 438.

2.1.4 The *frame* dimension

The *frame* dimension, as the term is used by Koops, refers to the (mostly) practical constraints on the research.[336] The major constraint of this enquiry is in its nature as a doctoral study carried out by a sole researcher with university-imposed time and word limits, which has led to significant scope limitations. Major scope limitations of this dissertation are set out in **section 5.4** of **Chapter 1**.

2.1.5 The *normative outlook* dimension

As Koops argues, normative outlooks underlying technology regulation are important to regulatory outcomes but are often not expressly incorporated into analyses.[337] The *normative outlook* of a research project can also influence choice of location along all of the other dimensions. As set out in **Chapter 1,** the normative outlook of this dissertation is one primarily focussed on the protection of consumers against possible misconduct by commercial entities.

In line with that normative stance, **section 4** of this chapter sets out the goals of the relevant law as a framework by which to judge the adequacy of existing legal rules, and identify any legal problems, arising out of the technology type under examination. However, due to *frame* constraints, a detailed analysis of the adequacy of these goals is not possible.

2.2 Other dimensions

The location of this enquiry in relation to Koops' other dimensions – those of *problem, knowledge, time, innovation* and *place* - requires a more detailed explanation. Therefore, an illustration of current thinking on some of the general concepts surrounding the study of law and technology follows below.

[336] Ibid (n 145) 320.

[337] Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 317.

2.2.1 The *problem* dimension

Unsurprisingly, the *problem* being addressed by the research forms an essential part of any map of the research space.[338] As set out in **section 3** of **Chapter 1,** the problem addressed by this dissertation is a practical one, that is, the extent to which legal problems may arise in the face of sociotechnical change enabled by a particular technology type, that of eObjects and the systems in which they participate. The significance and contribution of research into this particular problem was outlined in **section 4** of **Chapter 1**. Despite the practical nature of the problem, some of the general conceptual tools and terminologies proposed by scholars looking at law and technology issues can be of assistance in navigating the research space and constructing problem definitions. Those key concepts are sociotechnical change, the challenge of regulatory connection, and technological neutrality.

2.2.1.1 Sociotechnical change

> The current state of technology limits, in practice, what actions we *can* perform, what objects we *can* create, and what relationships we *can* form. It is thus common for technological change to impact the law, which limits what actions we *may* perform, what objects we *may* create and use, and what relationships *will* be recognized.[339]

The first important concept to be understood is the notion of sociotechnical *change*, as a technology by and of itself does not give rise to new legal problems.[340] This notion has been referred to by different names, including 'technological change',[341] 'socio-technological change'[342] and 'sociotechnical

[338] Ibid 319.

[339] Lyria Bennett Moses, 'Why Have a Theory of Law and Technological Change?' (2007) 8 Minnesota Journal of Law, Science & Technology 589, 594.

[340] Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 576–84.

[341] For example, Suvi Borgström and Volker Mauerhofer, 'Developing Law for the Bioeconomy' (2016) 34 Journal of Energy & Natural Resources Law 373.

[342] Ines Langemeyer, 'Contradictions in Expansive Learning: Towards a Critical Analysis of Self-Dependent Forms of Learning in Relation to Contemporary Socio-Technological Change' (2006) 7 Forum: Qualitative Social Research Art 12.

change'.[343] Definitions of 'technology' have been the subject of some discussion by theorists,[344] but the classification of eObjects as a manifestation of a 'technology' is uncontroversial. What should be noted is the importance of the 'social' dimension when considering change brought about by developments in technology. This reflects the reality that change in technology is brought about by social and political processes as well as technical ones, and the direction of change is shaped by human behaviours and presumptions underlying them.[345] These behaviours and presumptions reach well beyond any concept of a 'singular act of heroic invention'.[346] The path to particular technological developments is driven not just by technical discoveries but by particular human activities and preferences, and whether or not particular developments continue or fall by the wayside is equally driven by social factors.

This concept of 'sociotechnical change' used in this dissertation acknowledges that relevant change does not arise only in circumstances where a 'new' artefact or group of artefacts is created, or an existing artefact or group of artefacts is modified. 'Artefact', as used in this dissertation, includes 'all products of technology: … denot[ing] machines as well as technical processes, hardware as well as software'.[347] Sociotechnical change is

[343] For example, Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (n 127).

[344] For example, Donald A Schon, *Technology and Change: The New Heraclitus* (Delacorte Press 1967) 1; Ron Westrum, *Technologies and Society: The Shaping of People and Things* (Wadsworth 1990) 7; Brenner, *Law in an Era of 'Smart' Technology* (n 57) 8–9; Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172) 160–61, 165–67; Cockfield, 'Towards a Law and Technology Theory' (n 319) 384; Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 312.

[345] For example, Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (n 127); Hans K Klein and Daniel Lee Kleinman, 'The Social Construction of Technology: Structural Considerations' (2002) 27 Science, Technology, & Human Values 28; Donald MacKenzie and Judy Wajcman (eds), *The Social Shaping of Technology: How the Refrigerator Got Its Hum* (2nd edn, Open UP 1999).

[346] Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (n 127) 270.

[347] Ibid 291.

not confined to new artefacts, nor to products and processes capable of passing a 'novelty' test, such as that contained in patent law regimes.[348] It also includes new activities and new relationships enabled by technological developments.[349] Sociotechnical change can occur when new artefacts, conduct and/or relationships are made possible by the use of a new or modified technology, the use of an old technology in a new way (by the developers, those who commercialise the technology, downstream innovators, or end-users), or a significant increase or decrease in the scale of use of a technology.[350] It is also worth noting that 'old' things may be transformed into 'new' things where they are given new attributes. For example, 'refrigerators' and 'rubbish bins' are not new, but 'refrigerators and rubbish bins with data collection and communication capabilities' are, and therefore constitute a significant part of sociotechnical change.

Change in 'conduct' and 'relationships' are a particular focus in the examination of legal problems. Sociotechnical change can be readily identified in new forms of conduct enabled by new or modified technologies emerging to form part of social practice.[351] For example, the ready availability of smartphones and the creation of software that allows sharing of messages, photos and locations has led to profound changes in how human beings communicate with each other socially, and played some part in the creation of the 'gig economy'.[352] Sociotechnical change can also be seen in the creation of new types of relationships. Some of these new relationships have

[348] For example, Patents Act 1990 (Cth) s 18(1)(b)(i).

[349] Bennett Moses, 'Why Have a Theory of Law and Technological Change?' (n 339) 594.

[350] Koops, 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' (n 145) 313.

[351] Colin Tapper, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology' (1989) 15 Monash University Law Review 219, 225–26; Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5 Law, Innovation and Technology 1, 10.

[352] Gig economy refers to 'an economy in which individual workers are employed on a contract to do a particular task for a set time, with little connection to their employer, as dog walkers, people who do food shopping and deliveries, drivers in ride-sharing services, etc'. Butler, *Macquarie Dictionary: Australia's National Dictionary Online* (n 5).

been legally recognised, such as new types of 'parent' in the context of artificial reproduction technologies.[353] Recognition of other new relationships brought about by sociotechnical change is still the subject of substantial debate, such as continuing discussions around the potential for granting machines or software systems with autonomous decision-making capabilities separate legal personality.[354]

2.2.1.2 Regulatory disconnection and legal problems

Where sociotechnical change is significant, it is well-accepted that such change is likely to create challenges for existing legal frameworks. Questions about how law (and other regulatory tools) should respond to changing social and technological conditions will inevitably arise. In particular, should the new conduct, artefacts and/or relationships brought into being be permitted, prohibited, encouraged, required[355] or limited in some way? And if so, how?

Where legal rules are implemented or propounded by parliaments and judges to help in managing permissions, prohibitions, encouragements, requirements or limitations, this requires the examination of existing legal rules against desired outcomes. A mismatch between those rules and outcomes can give rise to a situation Brownsword calls the 'challenge of regulatory connection', or 'regulatory disconnection'.[356] This concept of regulatory disconnection encompasses the discrepancies between existing

[353] Family Law Act 1975 (Cth) s 60H. See also Lyria Bennett Moses, 'Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization' (2005) 6 Minnesota Journal of Law, Science & Technology 505, 529.

[354] For example, Giovanni Sartor, 'Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents' (2009) 17 Artificial Intelligence and Law 253; Paulius Čerka, Jurgita Grigienė and Gintarė Sirbikytė, 'Is It Possible to Grant Legal Personality to Artificial Intelligence Software Systems?' (2017) 33 Computer Law & Security Review 685; Migle Laukyte, 'Artificial Agents Among Us: Should we Recognize Them as Agents Proper?' (2017) 19 Ethics and Information Technology 1; Vladeck, 'Machines Without Principals: Liability Rules and Artificial Intelligence' (n 156).

[355] Brownsword, *Rights, Regulation, and the Technological Revolution* (n 18) ch 6.

[356] Ibid. The challenges of regulatory connection and disconnection are discussed in detail in Chapter 6.

law and other regulation created to order a previous sociotechnical environment, which then requires 'reconnection' with new actions, products and relationships made possible by new technologies.[357] Legal problems are uncovered in the discrepancies appearing in and around existing legal rules. The perception that such discrepancies regularly appear in the face of sociotechnical change has been characterised as a concern that law inherently has problems 'keeping up' with sociotechnical change, sometimes referred to as the 'pacing problem'.[358] Brownsword's work considers other important regulatory challenges, such as those of regulatory legitimacy and effectiveness.[359] However, this dissertation focusses predominantly on regulatory *disconnection*, characterised by Brownsword as 'the outstanding generic challenge presented by new technologies'.[360]

Bennett Moses classifies legal problems that might arise from regulatory disconnection in the context of sociotechnical change into four categories:[361]

> (1) there may be a need to create special rules designed to ban, restrict, encourage, or co-ordinate use of a new technology; ['**new harms or benefits**'][362]
>
> (2) there may be a need to clarify how existing laws apply to new artefacts, activities, and relationships, particularly where there is: 'uncertainty as to how a new activity, entity, or relationship will be classified; uncertainty where a new activity, entity, or relationship fits into more than one category, so as to become subject to different and conflicting rules; uncertainty in the context of conflicts of laws;

[357] Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (n 351) 7.

[358] See for example, Marchant, Allenby and Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (n 18).

[359] Brownsword, *Rights, Regulation, and the Technological Revolution* (n 18) chs 2–4 (regulatory legitimacy), ch 5 (regulatory effectiveness).

[360] Ibid 287.

[361] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 269.

[362] See also Jonathan Morgan, 'Torts and Technology' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017) 527–28; Mandel, 'Legal Evolution in Response to Technological Change' (n 319) 225.

> and uncertainty where an existing category becomes ambiguous in light of new forms of conduct' ['**uncertainty**']
>
> (3) the scope of existing legal rules may be inappropriate in the context of new technologies; ['**under- or over-inclusiveness**'] and
>
> (4) existing legal rules may become obsolete, where the conduct regulated is no longer undertaken, or the underlying facts have changed which means the rule is no longer justified, or where the rule has become 'prohibitively difficult to enforce';[363] ['**obsolescence**']

Generally, classification schemes such as this have been praised for providing a strong basis for legal knowledge, and for having practical significance in in aiding courts to achieve the 'most elementary requirement of justice: treating like cases alike'.[364] More particularly, a requirement that any problem uncovered be placed in an identified category (or in some cases, categories) assists in ensuring that any legal problems identified are specific and defined. The approach is based on the premise that some changes in the sociotechnical landscape will **not** give rise to regulatory disconnection. Even those which do to some extent create regulatory disconnection will not create problems in all of the above four categories.[365] The approach also actively discourages any assumptions that just because a technology is new, it automatically generates uncertainty or a need for new rules.[366] All of these

[363] See also Mandel, 'Legal Evolution in Response to Technological Change' (n 319) 268. The difficulties of enforcement in a world with a plethora of eObjects and related systems is extensively discussed in Mireille Hildebrandt's work on 'ambient law': see in particular, Hildebrandt and Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (n 240); Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172).

[364] Stephen A Smith, *Contract Theory* (OUP 2004) 45–46. See also Peter Birks, 'Definition and Division: A Meditation on Institutes' in Peter Birks (ed), *The Classification of Obligations* (OUP 1997); Mandel, 'Legal Evolution in Response to Technological Change' (n 319) 227–28.

[365] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 246.

[366] Ibid 252.

requirements reduce the likelihood that there is an overreaction to sociotechnical change.

2.2.1.3 Pitfalls of technological neutrality

In 2012, the Full Court of the Australian Federal Court stated in *National Rugby League Investments Pty Ltd v Singtel Optus Pty Ltd* that '[t]he desirability of technological neutrality of not limiting rights and defences to technologies known at the time when those rights and defences were enacted has been acknowledged for some time'.[367] (This statement was made in the context of the Copyright Act 1968 (Cth).) However, while the concept is commonly discussed in the context of legislative drafting, its relevance is not confined to this situation, but also to the development of common law rules. For example, in the High Court case of *Dow Jones & Co Inc v Gutnick*, Kirby J argued that common law rules should in general be 'technology-neutral', in that 'it is undesirable to express a rule of the common law in terms of a particular technology'.[368] The desire for technological neutrality has been advocated by lawmakers and policy organisations in a number of jurisdictions.[369]

Scholarly and policy arguments supporting the principle tend to cluster around three themes:

[367] *National Rugby League Investments Pty Ltd v Singtel Optus Pty Ltd* [2012] FCAFC 59 [95].

[368] *Dow Jones & Co Inc v Gutnick* [2002] HCA 56 [125].

[369] See for example, Explanatory Memorandum, Copyright Amendment Bill 2006 (Cth); Copyright Amendment (Digital Agenda) Act 2000 (Cth); United States, White House, 'The Framework for Global Electronic Commerce: Read the Framework' (July 1997) <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html> accessed 24 April 2019; OECD, 'Council Recommendation on Principles for Internet Policy Making' (13 December 2011) <www.oecd.org/internet/ieconomy/49258588.pdf> accessed 14 October 2015; Directive 2002/21/EC of the European Parliament and of the Council on 7 March 2002 on a common regulatory framework for electronic communications networks and services [2002] OJ L108/33.

1) consistency, equivalence, or non-discrimination, that is, treating like *effects* alike, even when the technology used to produce those effects is different;[370]
2) durability, futureproofing or statutory longevity, that is, ensuring that the law 'keeps up' with or even anticipates sociotechnical change;[371] and
3) criticisms of legislative bodies who and processes which move too slowly or lack capacity to understand new technologies.[372]

It is not difficult to find examples of where excessive technological specificity has led to problems, particularly where undesirable behaviours enabled by new forms of technology are excluded from the application of legislation due to the under-inclusiveness of definitions.[373] However, the nature and desirability of 'technological neutrality' itself is not without controversy. The concept has been explained in different ways, with conflicting meanings.[374] As a consequence, it has been criticised as 'insufficiently precise'[375] and 'poorly understood'.[376] Some attempts at implementation have been

[370] Reed, 'Taking Sides on Technology Neutrality' (n 140) 276; Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' (2010) 88 Texas Law Review 1685, 1691–92; Brad A Greenberg, 'Rethinking Technology Neutrality' (2016) 100 Minnesota Law Review 1495, 1513.

[371] Bert-Jaap Koops, 'Should ICT Regulation Be Technology Neutral?' in Bert-Jaap Koops and others (eds), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (TMC Asser Press 2006) 87–89; Reed, 'Taking Sides on Technology Neutrality' (n 140) 275–76; Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' (n 370) 1692–93. See also *Dow Jones & Co Inc v Gutnick* [125], where Kirby J used the postal acceptance rule as an example, and cited Hill, 'Flogging a Dead Horse: The Postal Acceptance Rule and Email' (2001) 17 Journal of Contract Law 151.

[372] Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' (n 370) 1694; Greenberg, 'Rethinking Technology Neutrality' (n 370) 1513.

[373] For example, see the discussion of the Spam Act in **section 3.5.2** of **Chapter 6** of this dissertation and Rebecca Giblin, 'Stranded in the Technological Dark Ages: Implications of the Full Federal Court's decision in NRL v Optus' (2012) 35 European Intellectual Property Review 632.

[374] Reed, 'Taking Sides on Technology Neutrality' (n 140) 265; Koops, 'Should ICT Regulation be Technology Neutral?' (n 371) 81–90.

[375] Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 585.

[376] Greenberg, 'Rethinking Technology Neutrality' (n 370) 1498.

censured as ineffective or undesirable.[377] A number of scholars have criticised its use as a general principle, and have argued on various grounds that in some circumstances technologically *specific* rules will better achieve desired outcomes.[378] Amongst these grounds, one particularly worth noting for this dissertation's purposes is Greenberg's argument (in the context of copyright law) that technological neutrality has the potential to amplify rather than reduce uncertainty in the interpretation of particular provisions, especially as a rule ages.[379]

The flexibility of the common law system allows considerable capacity for judges to apply old principles to new technologies. For example, Morgan argues that 'the common law of torts can, and will, adapt itself to new technologies as they arise',[380] and this is true in many circumstances. However, he continues on to ask the normative question of whether it *should* be allowed to do so in all cases, or be replaced with other regimes. He raises the specific problem of the potential of tort liability to stifle innovation in areas that governments wish to promote. Further regulation to mitigate the effects of the common law may then, Morgan suggests, be appropriate.

However, the problem goes deeper than an argument that the spectre of tort liability might discourage the development of new technologies and markets. The question must be asked as to whether attempts to continually expand the interpretation of general legal principles to emerging sectors, in circumstances where those principles emerged in reaction to a vastly different context, can have the effect of overstretching existing doctrines

---

[377] Reed, 'Taking Sides on Technology Neutrality' (n 140) 275–82; Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 586; Greenberg, 'Rethinking Technology Neutrality' (n 370) 1497. See also Kayleen Manwaring, 'A Shift in Time Saves No-One: Mobile Technologies and the NRL v Optus Decision' (2012) 5 Journal of the Australasian Law Teachers Association 83.

[378] Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 585–87; Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' (n 370) 1700–13; Reed, 'Taking Sides on Technology Neutrality' (n 140) 284; Greenberg, 'Rethinking Technology Neutrality' (n 370) 1500.

[379] Greenberg, 'Rethinking Technology Neutrality' (n 370) 1529–36.

[380] Morgan, 'Torts and Technology' (n 362) 540.

beyond manageability or sense. This overstretching may occur either in the context of general common law rules or in judicial interpretation of 'technologically neutral' legislative provisions. One example of this in the common law context has been exemplified by Kim and Radin in relation to the US cases on online contracts. In 2014 Kim published a substantial investigation of wrap contracts.[381] She concluded that a significant distortion of doctrine, particularly around constructions of consent from mere notice, has arisen due to the US courts' desire to enforce traditional contract law on new forms of contracts.[382] Radin has come to similar conclusions as a result of her detailed examination of boilerplate and standard form contracts.[383] Radin further argues that this 'doctrinal distortion' has led additionally to 'normative degradation, meaning it gets farther and farther away from the normative basis of contractual obligation'.[384] Mandel[385] makes a similar argument in a narrower context: that of the application of the common law doctrine of 'trespass to chattels' to a mass spammer at the suit of an Internet service provider, in the case of *CompuServe Inc v Cyber Promotions Inc.*[386]

The examples above reflect a significant problem potentially arising in regard to overzealous or ill-considered applications of the principle of technological neutrality. This problem is that well-meaning judicial attempts to apply *existing* laws to new things, conduct and relationships, where the existing law and its goals and purposes, are framed against a different sociotechnical context, may lead to perverse outcomes. In the words of the old legal adage: 'hard cases make bad law'.[387]

[381] Kim, *Wrap Contracts: Foundations and Ramifications* (n 39).

[382] Ibid 212.

[383] Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (n 39).

[384] Margaret Radin, 'The Deformation of Contract in the Information Society (2016 HLA Hart Memorial Lecture)' (2017) 37 Oxford Journal of Legal Studies 505, 522. See also Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (n 39) ch 2.

[385] Mandel, 'Legal Evolution in Response to Technological Change' (n 319) 232–33.

[386] *CompuServe Inc v Cyber Promotions Inc* 962 F Supp 1015 (SD Ohio 1997).

[387] *McHale v Watson* [1966] HCA 13 [16].

2.2.2 The *knowledge* dimension

In terms of the *knowledge* dimension, the enquiry in this dissertation concentrates on the 'known unknowns', or at least on the boundary between these and the 'known knowns'.[388] **Chapter 2**, as well as the Vignettes in **Chapter 4**, set out the nature of known sociotechnical change. What is also known – or at least suspected – that sociotechnical change arising out of eObjects will cause regulatory disconnection. The extent to which this will happen, and the specific nature of the disconnection, is the 'unknown' to be investigated in this enquiry, and the results of that investigation are set out in **Chapters 5** and **6.**

2.2.3 The *time* dimension

When considering regulatory disconnection in the face of sociotechnical change, the relevance of the *time* dimension is significant. Changes to the law or other forms of regulation should be approached cautiously. Failure to prohibit particular activities may lead to socially undesirable results,[389] such as allowing unlimited surveillance of private spaces. However, 'premature, over-reaching or excessive lawmaking may … be an option worse than doing nothing', particularly where investment in beneficial new technologies may be unnecessarily fettered or driven offshore by regulatory interference and compliance costs,[390] a problem not confined to Australia but apparent in many countries with sophisticated (and complex) business regulation regimes.

However, the speed of change and the timing of legal and other regulatory responses is important in successful reconnection. The need to address

[388] Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 318. See also United States, Department of Defense, 'Secretary Rumsfeld and General Myers' (DoD News Briefing, 12 February 2002) <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=2636> accessed 14 March 2017.

[389] Michael Kirby, 'The Fundamental Problem of Regulating Technology' (2009) 5 The Indian Journal of Law and Technology 1, 11.

[390] Ibid 12.

regulatory disconnection in a timely manner is drawn out by examination of the potential effects of what has been labelled the 'Collingridge dilemma',[391] or as Collingridge himself described it, the 'dilemma of social control'.[392] The Collingridge dilemma recognises that in some cases:

> potential benefits of new technology are widely accepted before enough is known about future consequences or potential risks to regulate the technology from the outset, while by the time enough is known about the consequences and possible harms to enable regulating it, vested interests in the success of technology are so entrenched that any regulatory effort will be expensive, dramatic and resisted.[393]

However, the possible negative results of the Collingridge dilemma may dictate a need to respond to technologies as they emerge, while still developing and well before coming into commercial use. Once a technology has been fully developed, there is usually a strong incentive by developers (and investors) to resist any regulatory change. The expense of changing technological design, and the likelihood that this will be passed onto customers, is the reason usually put forward to regulators for this resistance. Therefore, in some cases it may make sense to implement new laws before the technology is fully developed and/or the risks are fully known.[394] The speed of change reflected by the number of eObjects currently in commercial use and in advanced prototype means that the challenges posed by the Collingridge dilemma are real and immediate.

---

[391] Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (CUP 2012) 132; Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (n 351) 8.

[392] David Collingridge, *The Social Control of Technology* (Pinter 1980) 11.

[393] Morag Goodwin, 'Introduction: A Dimensions Approach to Technology Regulation' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010) 2.

[394] Gaia Bernstein, 'When New Technologies Are Still New: Windows of Opportunity for Privacy Protection' (2006) 51 Villanova Law Review 921; Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (n 351) 8.

2.2.4 The *innovation* dimension

Koops' *innovation* dimension is particularly important to consider when researching problems concerning technologies at a fairly high level of abstraction, as is the case in this dissertation. As a practical matter, a researcher will need to limit their scope in some way when dealing with a wide-ranging technology or set of technologies (see **section 5.4** of **Chapter 1**). Koops contends that non-innovative technologies are more likely to operate within existing regulatory frameworks than 'radically new technologies'.[395] Therefore, if a researcher wishes to explore the possibilities of regulatory disconnection, they are more likely to find fertile ground in innovative technologies.

However, Koops' notion of innovation is not narrowly confined. He also explains that 'innovation' is not confined to technologies that did not exist previously, but includes technologies which may have existed for some time, but where some form of change in the sociotechnical environment has led to them becoming far more widely used. He argues that '[i]t is far from rare that a change in the scale of a technology gives rise to significant regulatory questions'.[396] Therefore, innovation can be seen when an 'old' technology becomes significantly more popular, or is re-purposed to achieve different outcomes.

Understanding that changes in scale constitutes something 'new' or 'innovative' in the sociotechnical environment is important. Users of technology wishing to avoid additional or amended regulation have an incentive to argue that their conduct is not 'new', but the same as it always was. They may assert that the technology is just a tool to effect the same outcomes. However, a significant change in scale in the use of a technology may cause social change. This in itself may give rise to legal problems. In particular, an increase in the use of a technology can lead to greater

[395] Koops, 'Ten Dimensions of Technology Regulation: Finding your Bearings in the Research Space of an Emerging Discipline' (n 145) 313.
[396] Ibid.

effectiveness, and, as Mik argues, 'even if we are 'only' dealing with more extreme forms of 'old' commercial practices, their increased effectiveness in itself should raise legal concerns'.[397]

It is useful then in this dissertation to examine the innovations contained within or around eObjects in order to answer the research questions set out in **section 3** of **Chapter 1.** This dimension is of particular importance in research concerning eObjects. Some of the technology embodied in eObjects, such as Internet connectivity, may not be 'radically new', when compared with other innovations such as cloning or nanotechnology. However, as Koops suggests, a search for innovation should not be narrowly circumscribed to mere technical advances. eObjects provide a significant example of this. Vulkanovski pointed out that in many ways, the advent of eObjects did not bring anything 'entirely new to digital privacy and security concerns'.[398] Nevertheless, innovations in a range of areas relevant to eObjects will have a 'synergetic' effect on concerns that already existed in the 'conventional' digital environment,[399] namely:

1) Scale – … creat[ing] more data collection points, since more 'things' collect data;
2) Method – … creat[ing] novel ways of collecting data, such as via sensors and smart things;
3) Reach – … penetrating more intimate areas of our lives, such as data on our bodies and inside our homes; and
4) Nature – An advanced IoT ecosystem is designed to collect data covertly and 'in the background' via sensors and other digital tools, meaning that consumers may not be aware of the collection of personal information.

In this dissertation, the radical change in the scale, method, reach and nature of advertising and selling practices set out in **section 3.3.1** of **Chapter 5** and discussed further in **Chapter 6** provides another, more specific, example of this.

[397] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 22.

[398] Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63) 4.

[399] Ibid 5.

The technological developments of the third wave have resulted in a plethora of different devices and systems, working sometimes alone, and sometimes together, in a great variety of different environments. Therefore, it is not only the characteristics of the devices or systems themselves, but also the relationships between them, which give rise to significant innovations in the way human beings interact with the technologies. These innovations in turn can raise questions about how these interactions are and should be regulated. One illustration can be drawn from the interaction of the attributes of **mobility**, **adaptability** and **prevalence** in eObjects (described in **Chapter 2**). The prevalence of portable smart devices containing sensors, and the mobility of users interacting with smart environments with embedded sensors and communication links, mean that the places at which data might be captured have increased exponentially. The use of adaptable (or context-aware) devices means that a particular action by a user actually generates more data about that user than was previously the case. Such data includes, among other things, the where, when and how of user activities. This all means that there is a lot more data being captured, much of which is stored, mined, manipulated and disclosed to third parties.

Technical innovations found in eObjects are not the only innovations of relevance. How the technology is operationalised, applied and used in a functional sense is also important. The nature of the interaction between a user and a desktop computer is different from that of a user and a smartphone, and different again to that of a person driving past a traffic sensor embedded in a stop sign. The affordances – the things that can be done with eObjects (both intended and unintended) – will also be different. The differences are not just ones of overall design and functionality, but also of who or what is initiating and controlling the interaction. Also, *individual* attributes may not be the most relevant ones, as the *interaction* among attributes may give rise to the most interesting legal issues.

2.2.5 The *place* dimension

One of the key consequences of technological developments related to eObjects is the re-emergence of physical spaces and *places* as an important

concept in information technology.[400] Brownsword, Scotford and Yeung make the point that theoretical scholarship concerning 'law and information technology' is more well-established than scholarship in other areas of sociotechnical change.[401] It is true that such areas as Internet regulatory theory are fairly well-developed.[402] However, cyberspace scholarship has some limitations when researching eObjects and the systems in which they participate, due to its lack of emphasis on concepts of place and physicality.

When scholars and others talk about cyberspace, they tend to concentrate on its intangible aspects, its status as a mass 'consensus-hallucination'[403] rather than a physical space in which physical actions are carried out. Cyberspace has sometimes been conceived as a world without boundaries or physicality. It has even been argued that the word 'cyberspace' constitutes a positive denial of a physical place.[404] The role of the physical environment in conventional distributed systems is usually limited to acting as a conduit for power and communications, and as a repository for data storage and processing units.[405] The location of human users is often unimportant,

[400] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) ch 5; Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (n 144).

[401] Brownsword, Scotford and Yeung, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' (n 317) 3.

[402] See for example, John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (1996) 56 Humanist 18; David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367; Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet: Regulating Cyberspace* (Hart Publishing 1997); Lessig, *Code and Other Laws of Cyberspace* (n 334); Andrew D Murray, *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007); Dan Jerker B Svantesson, 'A Legal Method for Solving Issues of Internet Regulation' (2011) 19 International Journal of Law and Information Technology 243; Chris Reed, *Making Laws for Cyberspace* (OUP 2012).

[403] William Gibson, 'Burning Chrome' in *Burning Chrome* (Harper Collins 1995) 196–97.

[404] Roger Clarke, 'Paradise Gained, Paradise Re-Lost: How the Internet Is Being Changed from a Means of Liberation to a Tool of Authoritarianism' (2001) 18 Mots Pluriels. Also see Barlow, 'A Declaration of the Independence of Cyberspace' (n 402) 18.

[405] Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 8.

although not always, for example when state-sponsored censorship mechanisms are imposed on those living in a particular jurisdiction.[406]

While data communication via connectivity to the Internet or other internetworks is a core part of what makes up an eObject, eObjects are defined by much more than their connection to cyberspace. The physical location and form of many eObjects forms essential parts of their nature, and is inextricably linked to its use by humans.[407] For example, the ability of a mobile device to move quickly and easily in space between physical locations while maintaining functionality can significantly affect the nature and scope of its use. The impact of these issues on challenges for consumers is discussed in more detail in **Chapter 5**, particularly in **section 3.1.**

3 AN APPROACH TO UNCOVERING LEGAL PROBLEMS BROUGHT ABOUT BY EOBJECTS

In setting out the dimensions of the research, **section 2** of this chapter drew a map for the conceptual landscape. This **section 3** sets out the route taken in this dissertation to explore the landscape of the enquiry, and the reasons for that choice of route.

As discussed in **section 2.2.1.2** of this chapter, overreaction against sociotechnical change should preferably be avoided by scholars, legislatures and judges when examining legal implications. It is important for legal scholars to remember that most sociotechnical change does not emerge in a regulatory vacuum, particularly in the light of often forceful or fearful reactions by the public or interest groups or politicians to sociotechnical change. Just because a technology is new, or significantly changed, does not

[406] Such as the Great Firewall of China: see Bloomberg News, 'Quicktake: The Great Firewall of China' (*Bloomberg,* 6 November 2018) <www.bloomberg.com/quicktake/great-firewall-of-china> accessed 4 March 2019.

[407] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 109.

by itself mean that its applications operate outside of the scope of existing law.[408]

A new technology, especially in the ICT industry, is usually governed by at least some existing legal principles. For example, a new product is still usually subject to existing tortious principles and product liability legislation, those selling it subject to consumer protection and competition law, and creators able to protect it under existing intellectual property legislation.[409] So in many circumstances, there is no need for legislators and judges to create new rules or amend existing ones. For example, there are no barriers to a judge applying section 154F (Stealing motor vehicle or vessel) of the Crimes Act 1900 (NSW) in a criminal prosecution involving an accused who steals a driverless smart car.

However, in other instances, application of existing law may become more difficult when the technology or the sociotechnical landscape changes. For example, if the driverless car is involved in an accident causing injury or property damage, this may give rise to considerable uncertainty. Attempts to apply tortious principles or existing accident liability statutes may cause difficulties for judges. For example, Hubbard argues that there are 'virtually insurmountable proof problems'[410] in liability claims relating to driverless cars. These problems are due to the complexity of the internal systems of driverless cars and their necessary interconnection with other complex things, such as other cars and infrastructure.[411] Others argue that traditional principles of liability are incompatible with the emergent properties of a driverless car's embedded algorithms.[412] If as a result of sociotechnical

[408] Mandel, 'Legal Evolution in Response to Technological Change' (n 319) 226; Bennett Moses, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (n 351) 9.

[409] Bennett Moses, 'Agents of Change: How the Law Copes with Technological Change' (n 140) 768.

[410] F Patrick Hubbard, '"Sophisticated Robots": Balancing Liability, Regulation, and Innovation' (2014) 66 Florida Law Review 1803, 1851–52.

[411] Ibid 1851–52. See also Morgan, 'Torts and Technology' (n 362) 17–18.

[412] Erica Palmerini and others, *Robolaw – D6.2: Guidelines on Regulating Robotics* (2014) 23.

change the application of existing law is uncertain or would lead to a perverse result, then a true disconnection exists, and a case for 'reconnection': that is, the creation of new rules or a change to existing rules.

This is not to say that an initial disconnection means that law will always be disconnected from sociotechnical change. Both legislatures and judges have historically and more recently acted to adapt or clarify the law to respond to sociotechnical change. For example:

- in 1846, the NSW legislature created a new tortious suit of 'wrongful death' in response to the introduction of railways and other technologies of the industrial revolution;[413]
- in 2006, an Australian Federal Court judge clarified the common law for e-commerce transactions by expressly stating that a 'click' on a button on a website constituted 'a contract in writing signed by the parties';[414] and
- in 2008, the Australian Federal Parliament amended the definition of 'parent' to include non-biological parents where artificial conception technology is used.[415]

Section 2.2.1.2 of this chapter discussed Bennett Moses' classification scheme for legal problems arising from sociotechnical change. In addition to this scheme, Bennett Moses also proposed an approach to reviewing the existing legal landscape to assess what, if any, legal problems had arisen or would likely arise from specific types of sociotechnical change. This approach, or 'algorithm', requires the researcher to:

1) identify each new artefact, activity and relationship enabled by the technology under study;
2) identify the existing law (both common law and statutory rules) that already applies to the technology;

[413] Fatal Accidents Act 1846 (9 & 10 Vict c 93). See Barbara Macdonald, 'Legislative Intervention in the Law of Negligence: The Common Law, Statutory Interpretation and Tort Reform in Australia' (2005) 27 Sydney Law Review 443, 447–48.

[414] *eBay International AG v Creative Festival Entertainment Pty Ltd* [2006] FCA 1768 [49]. See further Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (n 36) 7.

[415] Family Law Act 1975 (Cth) s 60H.

3) identify the goals or purposes of those rules (to the extent they can be ascertained); and
4) measure the application of existing law to the new artefact, activity and relationship against the goals and purposes of the law,[416] to assess whether existing legal rules are obsolete, under or over-inclusive, uncertain, or *new* legal rules were needed to manage new risks or to encourage new behaviours.

The algorithm is intended to result in an identification of zero, one or more legal problems resulting from a failure of regulatory connection brought about by sociotechnical change.

This approach is generally followed in this dissertation, with some modifications. As Bennett Moses readily admits, such a rigorous approach applied to its fullest extent 'might take a professional lifetime'.[417] More limited analysis will often be necessary in order to make research practically possible. As a consequence, the algorithm has more significant *practical* utility as a 'checklist'[418] rather than in its full application, and methods for limiting the analysis must be found in order for it to be useful in uncovering legal problems. The limitation methods employed concerned the scope of rules and the description of the technology the subject of the enquiry.

This dissertation follows one of the methods of limitation suggested by Bennett Moses. The scope of legal rules examined[419] in this research project has already been narrowed as set out in **section 5.4.3** of **Chapter 1**. However, at the level of abstraction of the technology examined in this dissertation (discussed in **section 2** of **Chapter 2**), a further method or methods of limiting the analysis was required to make the research workable within the *frame* constraints of the doctoral study (see **section 2.1.4** of this chapter).

[416] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 282–84.

[417] Ibid 283.

[418] Ibid.

[419] Ibid.

One approach could have been to change the level of abstraction of the technology to a much finer-grained study, such as driverless cars, smart homes or agricultural applications of eObjects. Such research studies have their own importance, particularly where they are directed towards policy making or law reform in complex but narrow areas. However, this research project was driven by the *normative outlook* identified in **section 2.1.5** of this chapter, that of consumer protection. In particular, more general patterns of legal problems were sought to be examined that might apply to this large and diverse group, whose interests are often ignored in the initial stages of excitement about innovative technology.

It would have been impossible within the frame of this doctoral project to develop in full the algorithmic step of identifying all of the eObjects, conduct and relationships enabled by third wave technologies. So instead of further limiting the technology, this dissertation provides two things that act together as an approximation or stand-in for this process of full identification. The first and most important of these is the technical research framework developed in **Chapter 2.** The attributes and interactions set out in this framework are framed at a level of generality that attempts to be comprehensive. The word 'attempts' is necessary because a large portion of the technical research framework contained in **Chapter 2** is a list of 'other' attributes, based on what is commonly found in current manifestations of eObjects. What is 'common' in the technology is likely to change over time, as new uses are developed and old uses are abandoned. Change in use may also affect the interactions between the eObjects and other things and people.

The second contributor to the proxy is the set of Vignettes contained in **section 3.1** of **Chapter 4**. In contrast to the technical research framework developed in **Chapter 2**, no attempt has been made to make the Vignettes comprehensive. As discussed in **section 2.2** of **Chapter 4**, the Vignettes are used predominantly as an illustrative tool. However, those examining the Vignettes will be more readily able to visualise alternative use cases and circumstances where legal problems might exist for consumers. In larger research projects, the use of scenario studies (discussed further in **section 2.1**

of **Chapter 4** and **section 3.4** of **Chapter 8**) might provide a desirable alternative.

4 GOALS OF LAW REGULATING CONSUMER CONTRACTS

Section 3 of this chapter discussed the importance in the conceptual framework of identifying existing law, and its goals or purposes, as a starting place for any assessment of legal problems arising out of sociotechnical change. As set out in **section 2.1.5** of this chapter, the *normative outlook* of this dissertation concentrates on consumer protection. In line with that normative stance, and keeping to the narrow field of inquiry chosen within the *legal discipline* (set out in **section 2.1.3** of this chapter), this **section** sets out the goals of relevant consumer protection law. These goals provide a framework by which to investigate the main *problem* the subject of this dissertation: that is, judging the adequacy of existing legal rules, and identifying the likelihood of any regulatory disconnection arising out of the *technology type* under examination.

4.1 Goals arising out of the objectives of the ACL

In the field examined in this dissertation, the relevant law is that relating to consumer contracts. The law in Australia regulating consumer contracts, while originally based upon the common law of contracts, is heavily influenced by statute law designed to protect consumers against particular types of misconduct of commercial entities. The goals of this statutory framework provide good support for the *normative outlook* of this dissertation, focussing as it does on consumer protection (as discussed in **section 2.1.5** of this chapter). The articulation of clear goals in the supporting materials underlying this legislation also allows for the easier application of the approach to uncovering legal problems outlined in **section 3** of this chapter.

As discussed in **section 2.1.5** of this chapter**,** the *frame* of this dissertation does not allow for a significant discussion of the normative *adequacy* of the goals. Therefore, the research approach outlined in **section 3** of this chapter confines the uncovering of legal problems to the specific goals and purposes

of the actual law at hand, rather than any 'ideal' law of consumer protection. Nevertheless, a brief discussion of the limitations of these goals follows in **section 4.3**.

In 2008, the Productivity Commission issued its final report in its review of Australian consumer policy (**PC Consumer Policy Report**).[420] The government adopted this report as a 'detailed roadmap for consumer policy reform'.[421] The Ministerial Council of Consumer Affairs developed a reform package for Australian consumer protection law based on the PC Consumer Policy Report,[422] and in 2009, the Council of Australian Governments (**COAG**) signed the Intergovernmental Agreement for the Australian Consumer Law (**IGA**), which incorporated this reform package in an agreement to implement a 'a new national consumer policy framework to enhance consumer protection, reduce regulatory complexity for businesses and encourage the development of a seamless national economy.'[423] Because of this agreement and the associated referral of power by the states, the Commonwealth Parliament passed the Competition and Consumer Act 2010 (**CCA**). The CCA includes as its Schedule 2 a new national law on consumer protection, the ACL.

The IGA, adopting Recommendation 3.1 of the PC Consumer Policy Report, states that the overall objective of the new consumer framework is:

> to improve consumer wellbeing through consumer empowerment and protection, to foster effective competition and to enable the confident participation of consumers in markets in which both consumers and suppliers trade fairly.[424]

[420] Productivity Commission, *Review of Australia's Consumer Policy Framework* (Productivity Commission Inquiry Report No 45, April 2008).

[421] Commonwealth of Australia *Parliamentary Debates Second Reading Speech* House of Representatives 14 June 2009, 6981-90 (Craig Emerson) 6982.

[422] Ibid.

[423] Council of Australian Governments, *Intergovernmental Agreement for the Australian Consumer Law* (2009) Recital A.

[424] Ibid Recital C.

The IGA also adopted six 'operational objectives' from the PC Consumer Policy Report. These objectives were also included in the Explanatory Memorandum to the CCA.[425] This dissertation adopts the first *five* of these operational objectives as regulatory goals for consumer contracts, in addition to the goal of 'Choice' discussed in **section 4.3**. The six objectives are outlined below, and include the Productivity Commission's explanation of their meaning and nature.

These objectives are:

1) to ensure that consumers are sufficiently well-informed to benefit from and stimulate effective competition; ('**Information**')

   The overall objective of 'consumer empowerment' is directly linked with two specific policy aspirations relating to the provision of information: first, the need for effective *disclosure* linked to individual goods and services, and second, the need for effective general consumer *education* campaigns. Disclosure must be comprehensible (and tested to be so), and the detail should be layered consistent with consumer needs. Education campaigns should also be evaluated and tested. [426]

2) to ensure that goods and services are safe and fit for the purposes for which they were sold; ('**SafeFit**')

   In exploring this objective, the Productivity Commission concentrated on the costs involved for consumers and other members of society arising out of unsafe, poor quality and/or underperforming goods and services. Unsafe goods and services can give rise to physical and mental harms, individual and societal medical costs and economic loss such as lost wages and productivity.[427] Underperforming or poor quality goods and

[425] Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth) [23.7]–[23.8].

[426] Productivity Commission, *Review of Australia's Consumer Policy Framework* (n 420) Vol 2, Ch 11.

[427] Ibid Vol 2, 171-172.

services have effects on individual consumers, such as the cost of replacement goods, as well as potential damaging overall sales of goods and services due to general consumer mistrust.[428]

3) to prevent practices that are unfair; (‘**Fairness**’)

Most of the discussion of fairness undertaken by the Productivity Commission focusses on unfair contract terms, rather than unfair practices generally.[429] A series of ‘unfair practices’ are prohibited in the ACL, but there exists no general legislative or judicial definition of unfairness, so its precise limits are unknown.

In section 24 of the ACL, the majority (but not all) of the wording suggested by the Productivity Commission was adopted. In particular:

> (1) A term of a consumer contract … is unfair if:
>
> > (a) it would cause a significant imbalance in the parties' rights and obligations arising under the contract; and
> >
> > (b) it is not reasonably necessary in order to protect the legitimate interests of the party who would be advantaged by the term; and
> >
> > (c) it would cause detriment (whether financial or otherwise) to a party if it were to be applied or relied on.
>
> (2) In determining whether a term of a contract is unfair under subsection (1), a court may take into account such matters as it thinks relevant, but must take into account the following:
>
> > (a) the extent to which the term is transparent;
> >
> > (b) the contract as a whole.

[428] Ibid Vol 2, 172.

[429] Ibid Vol 2, Ch 7.

However, the ACL omits a number of recommendations of the Productivity Commission, in particular:

- section 24(1)(a) does not include the requirement that the significant imbalance is 'contrary to the requirements of good faith';
- section 24(1)(b) only requires a 'detriment', not a 'material detriment'; and
- section 24(2) does not contain an express requirement that the 'broader interests of consumers' are to be taken into account (although the wording of the section suggests that the court *may* take that into account if it thinks it relevant).[430]

It is arguable, therefore, that section 24 as drafted contains *stronger* protections for individual consumers than those recommended by the Productivity Commission.

4) to meet the needs of those consumers who are most vulnerable or are at the greatest disadvantage; ('**Disadvantage**')

A range of different definitions of 'vulnerable and disadvantaged consumers'[431] was canvassed in developing the operational objectives. Consolidating those definitions, the Productivity Commission stated:

> disadvantage can be seen as reflecting a set of (generally persistent) individual traits — such as poverty, low education, disability, or poor English proficiency — that increase the risk of a consumer experiencing detriment or/and intensify the adverse consequences of that detriment. … Vulnerability is a broader term relating to the susceptibility of consumers to detriment based on both their personal characteristics and the specific context in which they find themselves (market features, product attributes, the nature of the transaction, the regulatory environment)…it is best thought of as encompassing those at particular risk of being misled or making poor purchasing situations, either generally or in specific situations.[432]

[430] Ibid Vol 2, 168.

[431] Ibid Vol 2 Box 1.1, 13.

[432] Ibid Vol 2, 13.

However, the Productivity Commission concluded that 'neither vulnerability nor disadvantage can be defined precisely in terms of a *particular* risk of detriment'.[433] Importantly for the discussion of 'digital consumer manipulation' in **section 3.3.1** of **Chapter 5** and generally **Chapter 6** of this dissertation, the Productivity Commission did recognise that 'virtually all consumers can be vulnerable in some situations – so-called 'situational' vulnerability'. This recognition could imply that vulnerabilities that may not exist *ex ante*, but can be created or exacerbated by external factors, such as conduct by the supplier, are contemplated under this goal. This view is supported by provisions in the CCA directed specifically against inappropriate supplier conduct, such as undue harassment or coercion,[434] or undue influence.[435] However, despite this recognition, the majority of discussion in the PC Consumer Policy Report focussed on those with *pre-existing* vulnerabilities.

5) to provide accessible and timely redress where consumer detriment has occurred; ('**Redress**'); and

   Redress is defined as:

   > [c]ompensation or some form of amends for loss sustained by a consumer when markets fail to function properly… [r]edress arrangements should be … accessible, procedurally fair, proportionate, timely, and accountable, have no major gaps in coverage and be run efficiently.[436]

6) to promote proportionate, risk-based enforcement.[437]

   Difficulties of enforcement are deservedly part of the literature surrounding eObjects. However, because this is an expansive and

[433] Ibid Vol 2 Box 1.1, 13.

[434] ACL s 50.

[435] ACL s 22(1)(d).

[436] Productivity Commission, *Review of Australia's Consumer Policy Framework* (n 420) Vol 2, 192.

[437] Council of Australian Governments, *Intergovernmental Agreement for the Australian Consumer Law* (2009) Recital D.

complex topic on its own,[438] objective 6 is treated as being out of scope for this dissertation.

In addition to the goals or purposes of the ACL, there is one other important goal to be considered when assessing the adequacy of the law relating to consumer contracts. This is derived substantially from the common law of contract (although a similar goal exists in the civil law of European jurisdictions). This additional goal, which has been labelled '**Choice**' in this dissertation, is discussed in the next section.

4.2 Consumer Goal arising out of contract law

Helberger argues that the 'maintenance of autonomous choice' is a fundamental right of the individual consumer.[439] The United Nations Guidelines for Consumer Protection,[440] revised in 2015, also emphasised the importance of consumer choice, particularly 'informed choice … according to individual wishes and needs',[441] for its Member States. This choice, in its purest form, extends to a decision by a consumer as to with whom they wish to contract, the terms on which they contract, and whether they wish to contract at all. While the specific objectives of the ACL do not mention this goal expressly, the concept may be (weakly) inferred by the concepts of 'consumer empowerment' and the 'foster[ing of] effective competition' called upon in the IGA's overall objective.[442]

[438] See for example, Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172); Werbach, 'Sensors and Sensibilities' (n 58).

[439] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 140.

[440] United Nations Guidelines for Consumer Protection, GA Res 70/186, UN Doc A/RES/70/186 (adopted 22 December 2015). The Guidelines were first adopted by the General Assembly in resolution 39/248 of 16 April 1985, later expanded by the Economic and Social Council in resolution 1999/7 of 26 July 1999, and revised and adopted by the General Assembly in resolution 70/186 of 22 December 2015.

[441] Ibid 5, 8, 10.

[442] Council of Australian Governments, *Intergovernmental Agreement for the Australian Consumer Law* (2009) Recital C.

However, the idea that consumers should exercise free choice in entering into a contract was deeply embedded in Australian law relating to consumer contracts well before the ACL and its predecessor statutes. Carter, the eminent Australian contracts scholar, commences his opus on *Contract Law in Australia* with the acknowledgement that all Australian contract law is based on assumptions of 'freedom to decide whether to contract', as well as freedom to negotiate terms.[443] The High Court of Australia has taken a similar view, insisting that 'contractual obligations are voluntarily assumed'[444] and '[i]t is of the essence of contract, regarded as a class of obligations, that there is a voluntary assumption of a legally enforceable duty.'[445]

This concept is not confined to Australian contract law. As Mak states:

> Contract laws around the world recognise autonomy … as [a] general principle… underlying the specific rules of contract law. Autonomy is generally defined as the fundamental right of individuals to shape their own future through voluntary actions, and in private law translates into the freedom to decide with whom and on which terms to contract.[446]

[443] John W Carter, *Contract Law in Australia* (6th edn, LexisNexis Butterworths 2013) 8.

[444] *Astley v Austrust Ltd* (1999) 197 CLR 1, 1 (Gleeson CJ, McHugh, Gummow, Hayne and Callinan JJ).

[445] *Ermogenous v Greek Orthodox Community of SA Inc* [2002] HCA 8 [24] (Gaudron, McHugh, Hayne and Callinan JJ). See also *Australian Woollen Mills Pty Ltd v Commonwealth* (1954) 92 CLR 424, 457 (Dixon CJ, Williams, Webb, Fullagar and Kitto JJ).

[446] Vanessa Mak, 'Contract and Consumer Law' in Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee (eds), *Research Handbook in Data Science and Law* (Edward Elgar 2018) 5–6; WH van Boom and A Ogus, 'Introducing, Defining and Balancing "Autonomy v Paternalism"' (2010) 3 Erasmus Law Review 1.

The concept of a voluntary assumption of contractual obligations has also been supported by English,[447] US[448] and New Zealand scholars.[449]

That this concept is fundamental to contract law is supported by the major analytical (or descriptive) and normative theories proposed to underpin contract law.[450] Radin recently undertook a review of the major streams of contract theory, classifying both long-standing and more recent theories into four types: autonomy (rights) theories, welfare (economic) theories, reliance theories and equivalence of exchange theories.[451] There are some significant differences between the theories which make it difficult (if not impossible) to construct an uncontroversial list of *all* of the goals of contract law. However, Radin argues that 'all streams of philosophy of contract depend on a basic premise of voluntariness'.[452]

This is not to say that voluntariness or choice by the contracting parties is *unlimited*, in the theoretical frameworks, in the development of contractual doctrine, or in some specific legislative arrangements. For example, Kim acknowledges that approved *protections* for choice tend to be weaker in the welfare theories,[453] as they rely on the premise that contracts should be enforced because they maximise wealth[454] or other aspects of social welfare.[455] However, despite the weaker protections, Radin and other

[447] Andrew Burrows, *Understanding the Law of Obligations: Essays on Contract, Tort and Restitution* (Hart Publishing 1998) 13.

[448] Charles L Knapp, 'Rescuing Reliance: The Perils of Promissory Estoppel' (1998) 49 Hastings Law Journal 1191, 1333.

[449] Brian Coote, 'The Essence of Contract (Part II)' (1989) 1 Journal of Contract Law 183, 194–95.

[450] For an explanation of the difference between analytical and normative theories, see Smith, *Contract Theory* (n 364) 43–49.

[451] Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (n 39) 55–81.

[452] Ibid 57.

[453] Kim, *Wrap Contracts: Foundations and Ramifications* (n 39) 11.

[454] For example, Richard Posner, *The Problems of Jurisprudence* (Harvard UP 1990) 356–57; A Mitchell Polinsky, *An Introduction to Law and Economics* (4th edn, Wolters Kluwer Law & Business 2011) ch 5.

[455] For example, Daniel Markovits, 'Contract and Collaboration' (2004) 113 Yale Law Journal 1417, 1417.

scholars argue that the welfare theories nevertheless assume an element of choice by individuals, even if this is not stated explicitly.[456] As for doctrine, Robertson argues that judicial attitudes to standard form terms, objective approaches to formation, incorporation and interpretation, and default rules,[457] all challenge concepts of voluntariness. There are also some legislatively-derived obligations to contract, such as in the case of compulsory third-party car insurance.[458] Note, however, that many of the legal rules (in common law, equity and statute) relating to formation of contract appear to be based on maintaining the parties' voluntary choice to enter into a contract, such as the contractual requirement of mutual assent, and well-accepted common law and equitable contract formation defences, such as duress, incapacity, undue influence and unconscionable dealing.

This goal has many names: 'choice', 'freedom to contract', 'autonomy' and 'voluntariness'. For the purpose of this dissertation, it is labelled '**Choice**'. Collectively, objectives 1–5 listed above and the additional goal of **Choice** are referred to as the '**Consumer Goals**' in this dissertation. Therefore, the final list of Consumer Goals against which disbenefits to consumers are to be assessed is as follows: **Information**, **SafeFit**, **Fairness**, **Disadvantage**, **Redress** and **Choice**.

4.3 Limitations of the Consumer Goals

The United Nations' 2015 *Guidelines for Consumer Protection,*[459] are 'widely accepted as the international benchmark for good practice in consumer

[456] Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (n 39) 72; Christopher McMahon, 'iPromise: How Contract Theory Can Inform Regulation of Online Consumer Contracts' (2018) 21 Trinity College Law Review 174, 182; Smith, *Contract Theory* (n 364) 110.

[457] Andrew Robertson, 'The Limits of Voluntariness in Contract' (2005) 29 Melbourne University Law Review 179.

[458] Motor Accident Injuries Act 2017 (NSW) s 2.1(1).

[459] United Nations Guidelines for Consumer Protection, GA Res 70/186, UN Doc A/RES/70/186 (adopted 22 December 2015).

protection'.[460] These Guidelines contain a list of 'consumer needs' that are very similar to the goals of the ACL. These needs in the Guidelines also broadly reflect the 'consumer rights' promoted by Consumers International.[461] Consumers International is the international membership organisation for consumer groups, representing over 250 consumer organisations around the world and is a holder of General Consultative Status at the United Nations,[462] and their expressed vision is 'to empower and champion the rights of consumers, and ensure they are treated safely, fairly and honestly', reflecting the *normative outlook* of this dissertation.

Table 4: Consumer Goals, needs and rights

Consumer Rights (Consumers International)	**2015 Guidelines (United Nations)**	**Corresponding Consumer Goal**
	(III.5(b), IV.11(a)) Consumers who are vulnerable or disadvantaged should be protected	**Disadvantage**
Right to safety – 'To be protected against products, production processes and services that are hazardous to health or life'	(III.5(c), V.B, V.D) Consumers should be protected against threats to health and safety	**SafeFit**
	(III.5(d), V.C) Businesses should supply goods and services which are durable, reliable and fit for purpose	**SafeFit**
Right to be informed – 'To be given the facts needed to make an informed choice, *and to be protected against dishonest or misleading advertising and labelling*'	(III.5(d), IV.11(b), V.C) Consumers should be protected against unfair practices, such as misleading marketing practices and unfair contract terms	**Fairness**

[460] Consumers International, *Consumer Protection: Why It Matters to You: A Practical Guide to the United Nationals Guidelines for Consumer Protection* (2016).

[461] Consumers International, 'Frequently Asked Questions: What are the Consumer Rights?' <https://www.consumersinternational.org/who-we-are/faqs/#frequently-asked-questions-what-are-the-consumer-rights> accessed 10 September 2019.

[462] Consumers International, 'Who we are' <https://www.consumersinternational.org/who-we-are/our-history/> accessed 10 September 2019.

Consumer Rights (Consumers International)	**2015 Guidelines (United Nations)**	**Corresponding Consumer Goal**
Right to be informed – '*To be given the facts needed to make an informed choice*, and to be protected against dishonest or misleading advertising and labelling'	(III.5(e), IV.11(c)) Consumers should be given access to sufficient information to make informed individual choices	**Information Choice**
	(III.5(f), V.G) Consumers should be given access to education programmes	**Information**
Right to redress – 'To receive a fair settlement of just claims, including compensation for misrepresentation, shoddy goods or unsatisfactory services'	(III.5(g), V.F) Effective dispute resolution and redress should be provided to consumers	**Redress**
Right to choose – 'To be able to select from a range of products and services, offered at competitive prices with an assurance of satisfactory quality'		**Choice SafeFit**

However, the operational objectives contained in the IGA and Explanatory Memorandum (and consequently the Consumer Goals) do not include some of the more general consumer needs and rights promoted by the United Nations and Consumers International, and these are briefly outlined below.

Table 5: General consumer rights and needs

Consumer Rights (Consumers International)	**2015 Guidelines (United Nations)**	**Known as**
The right to be heard – 'To have consumer interests represented in the making and execution of government policy, and in the	III.5(h) Consumers should be given the freedom to form consumer groups which are allowed to present their views to decision-making bodies	**Representation**

Consumer Rights (Consumers International)	**2015 Guidelines (United Nations)**	**Known as**
development of products and services.'		
The right to a healthy environment –'To live and work in an environment that is non-threatening to the well-being of present and future generations.'	III.5(i), V.H Sustainable consumption by consumers should be promoted	**Sustainability**
The right to satisfaction of basic needs – 'To have access to basic, essential goods and services: adequate food, clothing, shelter, health care, education, public utilities, water and sanitation.'	III.5(a), V.E Consumers should have access to essential goods and services	**Essentials**
	III.5(j), V.I Consumers using electronic commerce should be given no less protection than is provided in other forms of commerce	**Parity**
	III.5(k) Consumers' privacy should be protected	**Privacy**

In Australia (similar to many other jurisdictions), generally the Privacy of consumers is dealt with separately in the Privacy Act. No specific principle of Parity exists in Australian consumer protection, but as the discussion of technological neutrality in **section 2.2.1.3** of this chapter indicates, both the judiciary and Parliament are often supportive of a similar principle. However, this attitude does not always prevail: for example, the regulation of unsolicited consumer agreements (discussed in **section 3.4** of **Chapter 6**) is highly technologically specific.

Representation by consumer groups and their right to be heard is generally entrenched in Australian policy-making processes, even when not

specifically expressed in legislation.[463] In fact, in some circles there is a concern that sometimes such groups were *over*-represented in policy debates, to the detriment of businesses.[464] However, the Productivity Commission nevertheless recommended that the government provide additional funding for consumer advocacy groups and consumer policy research, including a national representative consumer body and national policy research centre. However, a Treasury consultation on this recommendation in 2009 was not finalised,[465] and no national bodies with general consumer advocacy purposes have been funded by government, although some state government-funded and industry-specific Commonwealth-funded bodies exist.[466]

The most significant omissions from a normative perspective are in relation to the consumer needs for Essentials and Sustainability. The consumer need for Essentials is not embodied in a *general* right in Australia, but does appear as an industry-specific principle in relation to some utilities such as basic telecommunications services.[467] The political climate in Australia is such that any principle of Sustainability is seen infrequently and only as piecemeal industry-specific rules: such as restricting the use of single-use plastic shopping bags in some jurisdictions.[468] However, the omission of Essentials from the list of operational objectives and therefore the Consumer Goals is of some concern when it relates to eObjects: for example, see the discussion

[463] Productivity Commission, *Review of Australia's Consumer Policy Framework* (n 420) 275.

[464] Ibid 274.

[465] Treasury, *Consumer Voices: Sustaining Advocacy and Research in Australia's New Consumer Policy Framework* (May 2009) available at <http://archive.treasury.gov.au/contentitem.asp?ContentID=1532> accessed 12 September 2019.

[466] For example, the Consumer Policy Research Centre (<https://cprc.org.au/>) and the Consumer Action Law Centre (<https://consumeraction.org.au/>) in Victoria, and the national Australian Communications Consumer Action Network (ACCAN) (whose funding is provided by the Commonwealth government under section 593 of the Telecommunications Act 1997 (Cth), recovered from charges on telecommunications carriers (<http://accan.org.au/>).

[467] For example, under the Telecommunications (Consumer Protection and Service Standards) Act 1999.

[468] For example, Waste Reduction and Recycling Act 2017 (Qld) Ch 4 Pt 3A; Plastic Shopping Bags (Waste Avoidance) Act 2008 (SA).

concerning 'consumer lock-out' in **section 3.3.3** of **Chapter 5**. The omission of Sustainability is also concerning, as an upsurge in the manufacture of eObjects is likely to lead to a corresponding growth in e-waste problems.[469]

5 CONCLUDING REMARKS

The conceptual framework developed in this chapter, in combination with the technical research framework developed in **Chapter 2,** is then used in **Chapters 5**, **6** and **7** of this dissertation to analyse the potential for legal problems (and possible solutions) arising out of sociotechnical change brought about by the introduction of and growth in scale of the use of eObjects and the systems in which they participate. This chapter has located the research undertaken in this dissertation along ten dimensions of law and technology research, and has described how key concepts proposed by law and technology theorists might be used in this research.

The conceptual framework developed in this chapter also set out categories of legal problems that may arise in relation to sociotechnical change. It acknowledges that sociotechnical change does not emerge in a regulatory vacuum, and that measures must be taken against an overreaction to sociotechnical change. Rather, existing laws may apply, and they may be adequate, or they may be under- or over-inclusive, or uncertain, or obsolete, in the light of that change. It does not deny the possibility that *sui generis* rules may have to be created in order to deal with truly new devices, conduct or relationships, but urges rigour and caution in identifying these aspects of sociotechnical change.

The *technology type* examined in this dissertation is at a high level of abstraction, for the reasons set out in **section 2.1.1** of this chapter. Issues of

[469] Stacey Higginbotham, 'The Internet of Trash: IoT Has a Looming E-Waste Problem', (*IEEE Spectrum,* 29 May 2018) <https://spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem> accessed 7 September 2019; Josh Lepawsky, 'Beyond Recycling: solving e-waste problems must include designers and consumers' (*The Conversation,* 28 May 2015), <https://theconversation.com/beyond-recycling-solving-e-waste-problems-must-include-designers-and-consumers-41719> accessed 4 September 2019.

concern for consumers in relation to the sociotechnical change arising out of this technology type are still relatively unexplored. Therefore, it is necessary at first instance to identify the *innovations* arising from this sociotechnical change at a broad level, before attempting to uncover specific legal problems. Therefore, this dissertation provides in **Chapter 5** a broad analysis of consumer challenges arising from those innovations, and analyses how they might conflict with the underlying goals of Australian consumer protection law. Once conflicting challenges are identified, the next step dictated by the approach set out in **section 3** of this chapter is to then examine in detail the application of existing legal rules to each challenge.

This next step requires an in-depth doctrinal analysis of each challenge, and is performed in order to uncover the extent to which specific regulatory disconnection exists in relation to the new artefacts, conduct and relationships brought about by the advent of eObjects. An in-depth analysis of one challenge is carried out in **Chapter 6**, as the *frame* of this dissertation would not allow for doctrinal analyses of the other challenges. However, while the doctrinal analysis in **Chapter 6** can only provide useful insights into specific legal problems arising out of one challenge, the identified legal problems are not the only useful result of this dissertation. The analysis conducted in **Chapters 5** and **6** is also useful as a case study to examine the efficacy of the approach set out in this chapter.

Generally, the framework described in this chapter provided an essential and useful tool to answer the research questions posed by this dissertation. Some modifications required for the implementation of the framework in a practical way were described in **section 3** of this chapter. Additionally, as discussed in **section 3.3** of **Chapter 1**, 'reflecting back' on the case study in **Chapters 5** and **6** will reveal two other insights into the framework. The first of these relates to the possibility of the exposure or exacerbation of 'old' legal problems in the context of sociotechnical change. The second proposes a clarification of the concept of legal 'uncertainty'. These are discussed in detail in **section 2.2** of **Chapter 8**.

The research approach outlined in **section 3** of this chapter emphasises the importance of identifying the specific new artefacts, conduct and relationships enabled by a technology under study. The next chapter (**Chapter 4**) draws on the technical research framework outlined in **Chapter 2** to develop a series of Vignettes to illustrate how the attributes of and interactions between eObjects might manifest themselves to consumers in 'real life'.

Chapter 4 – eObjects in everyday life

1 AIMS OF CHAPTER

Chapter 2 set out in detail the sociotechnical change that is the subject of this dissertation. **Chapter 2** also developed a technical research framework which comprises a core concept, 'eObjects', with defined core and other attributes and interactions associated with it. However, it is difficult for many readers to understand the full scope of the impact of these technologies based on a list, however thoroughly and rigorously prepared. Additional assistance is required to better understand the full extent of sociotechnical change brought about by eObjects and the systems in which they participate, particularly how new forms of conduct and new relationships might be enabled by eObjects.

The required assistance is provided in this dissertation through the means of a series of Vignettes presented in **section 3** of this chapter. The Vignettes represent a circumscribed attempt to tell the stories of how people might live their lives in a world of eObjects. They form part of the proxy introduced in

section 3 of **Chapter 3** standing in for the unfeasible task of full identification of all of the eObjects, conduct and relationships enabled by third wave technologies. The Vignettes are intended to show how the attributes and interactions relating to eObjects previously identified in **Chapter 2** will impact the everyday life of consumers. The stories told in the Vignettes are intended to illustrate the analysis in **Chapters 5** and **6** of relevant challenges and legal implications. As set out in **section 3.2** of this chapter, the Vignettes are based on technology that is in current commercial use, or at least in advanced development. In this dissertation, the term 'Vignettes' with a leading capital is used to refer to the specific vignettes set out in **section 3** of this chapter, while 'vignettes' without a leading capital refers to vignettes in general.

2 A NARRATIVE APPROACH

2.1 Nature and justification

Chapter 3 explains the need for the identification of innovations and consequent legal problems in this study. In this dissertation, this identification is founded on the examination of the technical research framework outlined in **Chapter 2**. However, a series of Vignettes (set out in **section 3** of this chapter) has also been developed and used as an illustrative tool to examine what new things, activities and relationships might arise in relation to eObjects, and to explain more clearly what legal problems might arise as a result. The use of narrative vignettes shares both similarities and differences with the narrative approach by philosopher and legal scholar Hildebrandt in her 2015 exploration of how 'smart' technologies affect the rule of law in a democracy.[470]

In her book, Hildebrandt presented a fictional narrative entitled 'Diana in the Onlife World' (sic).[471] Hildebrandt built this narrative based on scenarios

[470] Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172).

[471] Ibid 1–8.

prepared as a result of a 5-year European research network study involving the collaboration of computer scientists, lawyers, social scientist and philosophers. A similar collaborative approach was used by the European Commission in relation to their research on ambient intelligence, halfway through the last decade, known as the 'SWAMI Project' (Safeguards in a World of Ambient Intelligence).[472]

Hildebrandt likened her methodology to that of scenario studies research, 'which aims… to assess future developments that are as yet uncertain but warrant an assessment of potential threats'.[473] This type of scenario studies approach is a valuable,[474] and possibly under-utilised approach to research into 'analys[ing] developments and changes in the recent past and elaborat[ing] on the possible and impossible for the near future'.[475] However, the not unreasonable insistence by scholars[476] that scenario studies research requires substantial and prolonged input by a range of interdisciplinary experts puts such an approach well beyond the *frame* of a doctoral project (as discussed in **section 2.1.4** of **Chapter 3**). Therefore, this dissertation

[472] See European Commission, Joint Research Centre, Information Society Unit, 'SWAMI Project: Safeguards in a World of Ambient Intelligence' (n 243); Wright and others (eds), *Safeguards in a World of Ambient Intelligence* (n 238).

[473] Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172) 8.

[474] See for example, R Rabbinge and M Vanoijen, 'Scenario Studies for Future Agriculture and Crop Protection' (1997) 103 European Journal of Plant Pathology 197; Joel Garreau, *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies – And What It Means to Be Human* (Doubleday 2005) 78–79 (detailing the use of scenario studies by public bodies such as Republic of Singapore, World Council on Sustainable Development, the US Central Intelligence Agency, and corporate entities such as Shell, IBM, Coca-Cola, Apple, Hewlett-Packard, AT&T, the California Energy Commission, Intel, Deutsche Bank, Heineken, Motorola and Nissan); Robert Power and others, 'Scenario Planning Case Studies Using Open Government Data' in Ralf Denzer and others (eds), *Environmental Software Systems: Infrastructures, Services and Applications* (Springer 2015).

[475] Rabbinge and Vanoijen, 'Scenario Studies for Future Agriculture and Crop Protection' (n 474) 198. This describes a subset of scenario studies referred to as 'analytic studies'.

[476] Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172) 8; Roger Clarke, 'Scenario-Based Research' (*Xamax Consultancy Pty Ltd,* 26 June 2003) <www.xamax.com.au/Res/Scenarios.html> accessed 22 August 2018 [7.1].

adopts a scaled-down approach, using vignettes instead of scenarios, that still serves the illustrative purpose of a narrative approach. As a result, steps needed to be taken in this dissertation to restrict the impact of problems created by the lack of an interdisciplinary expert model, and these are discussed further below in this section.

Vignettes are most commonly used in social science survey research[477] (including socio-legal research),[478] but they have also been used to develop clinical skills in other disciplines such as medicine.[479] In survey research, vignettes take the form of 'short stories about hypothetical characters in specified circumstances, to whose situation the interviewee is invited to respond.'[480] A vignette can also be described as a 'sort of "illustration" in words', such as a description of a hypothetical crime that was carried out by an imaginary perpetrator.[481]

Vignettes have been used in doctrinal legal research, although they are not usually labelled as vignettes, nor necessarily given any label at all.[482] The use of vignettes in doctrinal research reflects a long tradition of using the 'problem method' or 'case method' in the *teaching* of law.[483] In survey

[477] Christine Barter and Emma Renold, 'The Use of Vignettes in Qualitative Research' (Social Research Update 25, Summer 1999) <http://sru.soc.surrey.ac.uk/SRU25.html> accessed 25 November 2016.

[478] Philip Leith, 'A Note on Using Vignettes in Socio-Legal Research' (2013) 19 Web Journal of Current Legal Issues; Daniel Ho and others, 'A Comparative Survey of Legal Awareness between Hong Kong and Canadian Managers' (2013) 34 Company Lawyer 92.

[479] Leith, 'A Note on Using Vignettes in Socio-Legal Research' (n 478) 4.

[480] Janet Finch, 'The Vignette Technique in Survey Research' (1987) 21 Sociology 105, 105.

[481] Patrick Vargas, 'Vignette Question' in Paul J Lavrakas (ed), *Encyclopedia of Survey Research Methods* (Sage Publications 2011) 2 (online version).

[482] For example, Jerry Kang, 'Information Privacy in Cyberspace Transactions' (1998) 50 Stanford Law Review 1193; Brenner, 'Law in an Era of Pervasive Technology' (n 57); Kayleen Manwaring, 'Network Neutrality: Issues for Australia' (2010) 26 Computer Law and Security Review 630.

[483] For a discussion of the 'problem method' in legal teaching, see Gregory L Ogden, 'The Problem Method in Legal Education' (1984) 34 Journal of Legal Education 654, 654 and fn 1. For its use in doctrinal legal research by practitioners and students, see

research, a vignette is designed to evoke a response by a third party other than the researcher, and that forms an essential part of the definition. However, in their use in doctrinal research, the author responds rather than a third party. In doctrinal vignettes, the doctrinal researcher presents a short but (hopefully) rich situational description, then commonly responds to it by discussing the legal principles that might be applied by judges in that particular situation, as well as the consequences for the imaginary parties described in the vignette. The researcher may then move on to discuss whether or not these consequences are acceptable, to the researcher, to society, or to some other actors.

Unsurprisingly, law and technology literature often contains descriptions of *possible* futures.[484] However, the speculative nature of this practice has its detractors. Hildebrandt warned of problems at both extremes: the 'random … fantasies of Luddite techno-pessimists', versus unduly optimistic 'advertorials' by corporate (and government) enterprise often presented in lieu of 'serious evaluation of both threats and potential benefits'.[485] Beebe's influential critique of space law scholarship in 1999 highlighted some particular dangers around overblown attempts to 'legalise the future'.[486] He was concerned that space lawyers had a tendency to create problems to protect their own patch: that is, to argue against a possible future where law was redundant. Others have also expressed concern about the impact of

Terry Hutchison and Nigel Duncan, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83, 105.

[484] For example, Brenner, 'Law in an Era of Pervasive Technology' (n 57); Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172); Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63); House of Lords Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (n 130) 8–9.

[485] Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172) 8.

[486] Barton Beebe, 'Law's Empire and the Final Frontier: Legalizing the Future in the Early Corpus Juris Spatialis' (1999) 108 Yale Law Journal 1737.

'inflated predictions'[487] that may lead to 'risk mismatch[es]'[488] and subsequently less concentration on real problems,[489] as well as an emphasis on unnecessarily technologically-specific solutions.[490] This reflects Posner's earlier expressed concern in 1963 that the building of a system to analyse a future law led to 'empty conceptualising' and leaving the hard questions untouched.[491] The next section sets out the precautions taken in this dissertation to avoid these problems.

2.2 How the narrative approach is used in this dissertation

The Vignettes set out in **section 3** of this chapter have been developed to assist in illustrating the operation of the technical research framework set out in **Chapter 2**. The specific technology discussed in the Vignettes has been developed based on the empirical research undertaken in relation to the technologies outlined in **Chapter 2**, and their source is set out in **Table 4** in **section 3.2** of this chapter. The Vignettes are used in **Chapter 5** to illustrate the nature of the challenges for consumers arising from the attributes and interactions of eObjects and related systems, and how these challenges might lead to detrimental outcomes. A subset is also used in **Chapter 6** to further discuss the legal principles that might be applied by judges to the case of digital consumer manipulation, and the consequences for consumers. However, the analysis that follows in **Chapters 5** and **6** of this dissertation is not exclusively confined to the specific technologies in the Vignettes. Rather, the specific technologies have been chosen to illustrate combinations of attributes and interactions identified in **Chapter 2**.

[487] Lyria Bennett Moses, 'Regulating Beyond Nanotechnology' (2011) 30 IEEE Technology and Society Magazine 42, 43.

[488] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (revised and expanded edn, Mercatus Center at George Mason University 2016) 55.

[489] Ibid; Bennett Moses, 'Regulating Beyond Nanotechnology' (n 487) 43.

[490] See also Lyria Bennett Moses, 'Exploring Technological Frontiers: Autonomy in Legal Scholarship' (2010) 30 Bulletin of Science, Technology & Society 22, 24.

[491] Richard Posner, 'Law and Public Order in Space (Book Review)' (1964) 77 Harvard Law Review 1370, 1371.

Using the Vignettes in addition to the technical research framework has the potential to enhance a reader's capacity to understand the arguments presented.[492] It is uncontroversial to assume that a wider range of people will more readily understand and reflect on a story than on a list of attributes. The Vignettes will assist not only in understanding the analysis contained in the dissertation, but can aid in any role the dissertation may have to play in public policy debates.

The Vignettes in the following section are comprised of a series of hypothetical stories, with fictional names, places, and government programs. In line with the scope of this dissertation, the focus is on consumer applications of eObjects with a range of attributes and interactions. Although these specific instances are fictional, the Vignettes are primarily based on existing technology and known practices. This is done in order to limit the effect of the concerns raised in **section 2.1** of this chapter in relation to overly pessimistic or overly optimistic visions of the future. Not all of the technologies discussed are commercially available, but include those well-known to be subject to imminent commercial release or to be at an advanced stage of development, such as in the case of driverless cars. Unfortunately, publicly available and scholarly knowledge of 'behind-the-scenes' practices, data sharing models and proprietary technology is likely to be deficient due to intentional corporate secrecy policies.[493] Therefore, a certain amount of limited and modest speculation, primarily relating to the nature of business models and subsequent information sharing between commercial parties, is unavoidable.

An examination of more speculative technologies and practices could lead to interesting doctrinal discussions. However, these are not included in this dissertation for two reasons. First, to avoid the perils of 'inflated predictions' discussed in **section 2.1** of this chapter. Second, as the discussion of the *time*

[492] Roger Clarke, 'Instrumentalist Futurism: A Tool for Examining IT Impacts and Implications' (6 October 1997) <www.rogerclarke.com/DV/InstFut.html> accessed 24 November 2016.

[493] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard UP 2015).

dimension and the Collingridge dilemma in **section 2.2.3** of **Chapter 3** illustrates, analysis of existing or imminent sociotechnical change is more urgent, and an analysis of more speculative change based on one person's speculation is likely to be too premature to be helpful.

The next section sets out a series of Vignettes illustrating the new things, conduct and relationships enabled by eObjects and the systems in which they participate, and how they might affect consumers in their everyday lives.

3 eOBJECTS IN EVERYDAY LIFE

3.1 The Vignettes

It is recommended that the entire set of Vignettes in this section be read before the discussion in **Chapters 5** and **6**, to 'set the scene' for that discussion by outlining how consumers may live their everyday lives surrounded by eObjects. However, those chapters refer to each Vignette used in the discussion by the labels set out on the left-hand side of each Vignette below: for example, **Vignette J11**. Therefore, it is possible to read **Chapters 5** and **6** first, and refer back to each Vignette in this section by use of the label cross-referencing.

The labels attached to each Vignette have been derived from the first letter of the dominant fictional character (or fictional setting, in the case of the first Vignette), plus a serial number in sequential order. The footnotes attached to the Vignette labels reference where each Vignette is discussed in **Chapters 5** and **6** of the dissertation.

E1[494] *Everyware Place*

Everyware Place is a small apartment block with 8 flats in inner suburban Sydney, Australia. It is in a desirable location, close to a train station and a brand-new shopping centre. When the apartment block was completed a year ago, in 2020, buyers were attracted by the smart home installation that was offered with each flat. This installation was partly funded by the Greater Sydney Council as part of their Building Better Cities program. When the apartment block was first completed, Fahim and his cat Medusa moved into No 5, on the second floor. Jessica moved into No 7 across the hall with her then partner, Steve, and her daughter, Mylin. After a recommendation from Jessica, three months ago her friend Orana bought No 1 on the ground floor as an investment property. Orana's mother Kylie now lives in No 1 as Orana's tenant.

F1[495] *Fahim – Flat No 5*

Fahim usually catches the train to his work as a nurse in a big inner-city hospital. He has a car, but only uses it when he is working an evening shift. He is very careful about properly managing his Type I diabetes, so he tends to jog home every day he can, and tracks his exercise via his smart wristband. He also uses an Internet-connected insulin pump and continuous glucose monitor, and tracks the data via his smartphone.

F2[496] Fahim visits the local shopping centre every Saturday to check out the best bargains. He has an excellent smart phone, which he got offered at a discounted price in a promotion by the shopping centre administration. All he had to agree to was to download an app to his smartphone and he has found that pretty useful at identifying discounts.

[494] This sets up the background for the rest of the Vignettes and is not separately referred to.

[495] **Chapter 5, sections 3.1.3, 3.3.1, 3.4.1.1, 3.4.1.2.**

[496] **Chapter 5, section 3.3.1; Chapter 6, section 2.1.**

F3[497] He always carries his phone because he uses it to interact with his Internet-connected insulin pump. He is a bit annoyed, however, as they are not working well together since the latest security upgrade to the phone.

F4[498] Fahim is feeling tired and is almost ready to go home, when he gets a message on his phone just as he walks past Doughnuts & More! His favourite doughnuts are on special and he just cannot resist. He feels a bit guilty as he succumbed to a similar advertisement last week at about the same time.[499]

F5[500] While eating his pink-iced doughnut, he gets another notification on his smartphone. It offers a really good discount on a smart kettle that he has been eyeing for ages – and he is standing right outside a branch of the electronics store chain that is offering the discount.

Fahim is very pleased with his new purchase, as he got 50% off by just being in the right place at the right time (or so he thinks). However, once he gets home he gets a rude shock, as his kettle is incompatible with his smart home system. He takes it back to the shop straight away – but the sales assistant tells him no returns on sale items unless they are faulty. He will have to try and sell it on eBay.

F6[501] Later that afternoon he realises that his automated vacuum cleaner is stuck in the one place, and has not moved all day. There is cat fur all over the place. He turns it off and on again, but it is no good. He takes it to the local electronics shop for repair, as it is out of warranty. However, the repair person at the electronic shop has bad news for him. She thinks the fix is likely to be simple, but the problem appears to be in the cleaner's proprietary software. With the technological protection measures applied to it, only the manufacturer can make changes. Fahim is unhappy. He has had another device serviced by that manufacturer before, and it was very expensive.

[497] **Chapter 5, section 3.5.2.**

[498] **Chapter 5, section 3.3.1; Chapter 6, sections 2.1, 3.2.4, 3.2.5.**

[499] The doughnut example is taken from Calo, 'Digital Market Manipulation' (n 42) 995.

[500] **Chapter 5, section 3.5.2.**

[501] **Chapter 5, sections 3.1.4, 3.4.2.**

F7[502] The next evening, Fahim gets an urgent call from the hospital, asking can he do an evening shift beginning at midnight? He sighs – only two hours' notice seems to be par for the course – but he needs to replace his cleaner and the kettle, so he agrees. He runs down to the garage to his car, but it refuses to start. He rings his roadside assistance provider and they, luckily, make it to his house with an hour to spare. However, it is definitely not his lucky week. The mechanic tells him that the starter interrupt device (installed by the finance company who provided his car loan) has been activated. As far as Fahim knows, his instalment payment should have been debited from his bank account as usual the day before. He vaguely remembers hearing something on the news yesterday about his bank's online services being down. He tries to ring the bank and the finance company, but at 11pm he only gets through to voicemail. He eventually pays for a rideshare to the hospital, but his boss is unhappy as he is very late.

J1[503] *Jessica – Flat No 7*

Jessica runs her own residential building business. Most of her work is in the outer suburbs, so she travels many kilometres each day in her autonomous vehicle, which she has nicknamed Kitt (being a fan of 1980s TV shows). Six months after moving into Everyware Place, Jessica and Steve broke up, so now Jessica lives just with her daughter, Mylin.

J2[504] Unlike her neighbour, Jessica does not like shopping. However, since she has discovered Wulwurths AutoBuy, she does not tend to run out of toilet paper or washing detergent any longer. When she is close to needing a refill, she just clicks on the Internet-connected button next to her toilet or washing machine, and she gets a delivery the next day by drone. It is even easier to get her coffee refills, as her coffee machine has a reordering facility built in which automatically reorders when she is running out of coffee pods (although she cannot believe how expensive her refill bill usually is). Her smart refrigerator has a similar reordering facility for refrigerated products.

[502] **Chapter 5, section 3.2.**

[503] **Chapter 5, section 3.4.1.1.**

[504] **Chapter 5, sections 3.1.4, 3.4, 3.5.1.2.**

J3[505] On Saturday afternoon, after a particularly busy day, Jessica heads home. Her vehicle, Kitt notes that she is within 10 km of home, and asks if she wants coffee. By the time she gets into the flat, a cup has been brewed for her. She grabs it from the kitchen and sits gratefully on the couch. She calls out 'Max, can I watch the episode of *MacGyver* with the bomb and the paperclip?'. Max, her smart home hub and virtual personal assistant, communicates with her home theatre system and orders the retrieval of the relevant episode and turns on the television, closing the blinds and dimming the lights at the same time. Five minutes later, Max tells her that her shopping has arrived by drone and is in the secure parcel area downstairs. Jessica's coffee machine had ordered coffee pods earlier that day as she was running low.

J4[506] She keeps one eye on the television as she sorts through her files to find out who she needs to contact about her smart lock. After Steve moved out, he started showing up at the flat at odd hours. Eventually she sought an apprehended violence order, which prohibits him from coming within 100m of Everyware Place. However, Steve still has the administration password to the smart lock. The police have advised her that she needs to get that changed. Luckily, she got copies of all the house-servicing contracts Steve entered into. She finds the 'all hours' number for Smart Locks Pty Ltd. Unfortunately, it appears to be disconnected.

J5[507] The next day, Jessica comes home from the gym at midday and sees a fire engine outside Everyware Place. She finds to her horror that fire fighters are in her flat and her kitchen has severe fire, smoke and water damage. She is told by the fire fighters that her stovetop was left on. This is a great surprise as she never uses it (she always has takeaway for dinner). NSW Police's Cybersecurity Unit tells her that the new Internet-connected lamp she just bought has been reported with significant security vulnerabilities, and speculate that that someone has hacked into her smart home through the lamp, and turned on the stovetop. Luckily the hacker had not got to the smoke alarms, which were protected by an additional layer of security.

[505] **Chapter 5, sections 3.2, 3.3.1; Chapter 6, sections 2.1, 3.1, 3.3.3.**

[506] **Chapter 5, sections 3.1.5, 3.2.**

[507] **Chapter 5, sections 3.1.1, 3.5.4.**

J6[508] She is particularly stressed by this incident, as only last week she had a car accident on her way home from a site. She was in manual mode, which tended to work better on the back roads (Kitt often gets lost in rural areas), but momentarily lost control of her steering and brakes and veered into another car on the way home. She was at a loss to explain why this happened, as it appeared as if the car had a mind of its own. She used to tinker with cars with her mother when she was a teenager, so she has had a look at the car, but she cannot access the proprietary software without the password provided exclusively to authorised repairers.

J7[509] She is upset by the problems she has been having, and takes Kitt over to visit her friend Orana, who lives a couple of suburbs away. Orana commiserates with her over dinner and a bottle of wine. Jessica thinks she is fine to drive home, but her breathalyser lock on her smart car says no. Jessica is resigned to the fact that she will have to stay the night with her friend. This has happened a few times over the past six months – breaking up is hard to do.

J8[510] She thinks nothing more of the incident. However, a year later in family court proceedings Kitt's data is subpoenaed and Steve claims that she was regularly 'out of control' during the relationship. His lawyer puts the breathalyser data into evidence.

J9[511] On Monday morning Jessica walks into her bathroom and looks in the mirror. 'Ugh', she says out loud, 'look at all those wrinkles, I'm getting old'. She brushes her hair with the hairbrush that she was given by her hairdresser at her last visit, which glows red, indicating she is brushing her hair too hard, risking split ends. Max, her smart home hub and digital personal assistant, hears her but does not respond. Business has been a bit slow lately, so later that evening, Jessica asks Max to find and play a few clips on YouTube containing tips on marketing to potential clients. She notices in passing the lead-in ad for some form of beauty product.

[508] **Chapter 5, sections 3.1.1, 3.1.2, 3.4.2.**

[509] **Chapter 5, section 3.4.1.1.**

[510] **Chapter 5, section 3.4.1.1.**

[511] **Chapter 4, section 3.3, Chapter 5, section 3.3.1, Chapter 6, section 2.1, 3.2.3, 3.2.4, 3.4.**

J10[512] The next day, Jessica's 9-year-old daughter Mylin begs to go shopping for her birthday present. Max suggests the local shopping centre as the best place to go. As they enter the shopping centre, the interactive billboard near the front displays an ad telling the story of a vaguely familiar beauty product that magically transforms a somewhat down-at-heel looking middle-aged woman who just lost her job into a glamorous and successful CEO of her own consulting business.

J11[513] Jessica and Mylin go to the toy store, and Mylin knows exactly what she wants to get, including the brand, much to Jessica's relief as she is pressed for time. What Jessica does not know is that Mylin's birthday present was suggested by Ella, Mylin's Internet-connected doll. Mylin's father bought the doll in an attempt to get her interested in doing research for her school projects.

J12[514] As Jessica and Mylin start to walk towards the exit of the shopping centre, Jessica's smartphone pings – she has been offered a 10% discount on Couteux's new wrinkle cream – 'only $150 down from $200 for one week only!', and a 50% discount on Prix Eleve's dry hair conditioner. She makes a quick stop at the centre's pharmacy: it is still not cheap with the discount but at least she will get the rewards points.

J13[515] At 9:30pm, while Jessica is packing for an overseas work trip, Max reminds her of her sister's birthday tomorrow. She asks it to order her sister's favourite flowers. She is a bit horrified at the price, as she ordered the same flowers herself on a whim two weeks ago and she was sure she only paid half that! However, she confirms the order as she is out of time to think of anything else, and her sister has been calling a lot recently looking for support for her marital problems.

[512] **Chapter 5, sections 3.3.1, Chapter 6, sections 2.1, 2.2, 3.2.4.**

[513] **Chapter 5, sections 3.3.1, Chapter 6, sections 2.1, 2.2, 3.2.4, 3.3.3, 3.3.4, 3.5.4.1.**

[514] **Chapter 6, sections 2.2, 3.2.4, 3.2.5, 3.4.**

[515] **Chapter 5, section 3.3.1, Chapter 6, sections 2.1, 3.2.2, 3.2.4, 3.2.5.**

J14[516] Max also reminds her that her smartphone contract is due to expire, and quotes the price for a new 2-year contract, with a 10% increase in price. She asks hopefully 'Max, is there anything cheaper'? Max replies 'There are cheaper packages, but this is the one that best suits your likely needs and preferences'. She tells Max to approve the renewal, finishes her packing, and goes to bed.

K1[517] *Kylie – Flat No 1*

Orana's mother Kylie has had some significant health problems. She has had a pacemaker for about 8 years. Last year, she had a general-purpose health monitoring device installed so her GP and her daughter could keep an eye on her, but in her home town in rural South Australia the mobile connectivity was too patchy for it to be reliable. Orana has moved her to the city so that she can keep an eye on her.

K2[518] Kylie gets a notification on the container for her heart medication that she has forgotten to take her pills. It is a bit odd, as she could have sworn she took a couple of tablets a few hours ago. But her memory has not been that great lately, so she takes a couple more tablets.

K3[519] Kylie's watch, which she received as a present from her mother, has finally broken down after 50 years. She goes to the shopping centre to buy a new one, but comes home disappointed. There are only smartwatches available these days – unless you have a fortune to spend - and she does not want one of those. It is bad enough that her doctor and Orana know where she is all the time: she does not want some faceless corporate entity tracking her movements as well.

[516] **Chapter 5, section 3.3.1, Chapter 6, sections 2.1, 3.2.3, 3.2.4, Chapter 8, section 3.2.**

[517] **Chapter 5, sections 3.1.2, 3.3.3, 3.4.1.2.**

[518] **Chapter 5, section 3.1.3.**

[519] **Chapter 5, section 3.3.3.**

3.2 'Real-life' technology underlying the Vignettes

The Vignettes derive from lengthy monitoring and inspection of a variety of technical, policy and popular sources on various technologies and their potential applications. The technologies referred to are in current commercial use, or in advanced development. **Table 4** and its associated footnotes sets out 'real-life' examples of the technologies used in the Vignettes.

Table 6: Real-life technology underlying the Vignettes

Vignette	Vignette example	Actual example/source
E1	Building Better Cities Program	Australia, Department of Infrastructure, Regional Development and Cities, Smart Cities and Suburbs Program[520]
E1	Smart home installation	Smart Home Solutions[521]
F1	Smart wristband	Fitbit[522]
F1 + F3	Connected insulin pump and glucose monitor	Medtronic[523]
F2 + F4 + F5 + J12	Beacon technology	Beaconnected[524]
F5	Smart kettle	Firebox iKettle 3rd Gen[525]
F6	Automated vacuum cleaner	Neato Botvac Connected[526]

[520] Australia, Department of Infrastructure, Regional Development and Cities, 'Smart Cities and Suburbs Program' <https://cities.infrastructure.gov.au/smart-cities-program> accessed 23 August 2018.

[521] Smart Homes <www.smarthomes.com.au> accessed 24 August 2018.

[522] Fitbit (n 308).

[523] Comstock, 'Medtronic Launches Smartphone Connectivity for CGMs, Insulin Pumps' (n 162). See also Medtronic (n 189).

[524] Beaconnected <https://beaconnected.com.au/> accessed 23 August 2018.

[525] Firebox, 'iKettle: 3rd Gen' <https://www.firebox.com/iKettle-3rd-Gen/p8185> accessed 25 April 2019.

[526] Neato, 'Botvac™ Connected: The Ultimate Navigating Wi-Fi Connected Robot Vacuum' <www.neatorobotics.com/robot-vacuum/botvac-connected-series/botvac-connected/> accessed 23 August 2018.

Vignette	Vignette example	Actual example/source
F7	Starter interrupt device	PayTeck Starter Interrupt device[527]
J1 + J6 + J7 + J8	Self-driving car	Waymo[528]
J2	Wulworths AutoBuy	Amazon Dash[529]
J2 + J3	Smart coffee machine	Behmor Brewer[530]
J3	Connected home theatre system	Samsung Smart TV[531]
J3	Delivery drone	Amazon Prime Air Delivery[532]
J3	Connected blinds and lights	TSHX Intelligent lighting and blinds[533]
J4	Smart lock	August Smart Lock Pro + Connect[534]
J5	NSW Police Cybersecurity Unit	US Department of Justice Cybersecurity Unit[535]
J5	Internet-connected lamp	Good Night Lamp[536]

[527] Payteck, 'Welcome to Payteck' <www.payteck.cc/> accessed 24 August 2018.

[528] Waymo <https://waymo.com/> accessed 23 August 2018. See also Alex Davies, 'The Wired Guide to Self-Driving Cars' (*Wired*, 1 February 2018) <www.wired.com/story/guide-self-driving-cars/> accessed 23 August 2018.

[529] Amazon, 'Tide Dash Button: Save 5% on All Products Ordered through This Button' <www.amazon.com/Tide-Dash-Button-products-ordered/dp/B0187TMRYM/ref=sr_1_1?ie=UTF8&qid=1531363704&sr=8-1&keywords=amazon+dash+button> accessed 11 July 2018.

[530] Behmor <https://behmor.com/> accessed 25 August 2018.

[531] Samsung <www.samsung.com/us/explore/smart-tv/highlights/> accessed 25 August 2018.

[532] Amazon, 'Amazon Prime Air' <www.amazon.com/Amazon-Prime-Air/b?node=8037720011> accessed 25 August 2018.

[533] TSHX, 'Intelligent Lighting & Blinds' <www.tshx.com.au/light-blinds-automation> accessed 25 August 2018.

[534] August, 'Smart Lock Pro + Connect' <https://store.august.com/products/august-smart-lock-pro-connect?utm_source=5056&utm_medium=DIS&utm_campaign=a22-a325-a4020-07> accessed 24 August 2018.

[535] United States, Department of Justice, 'Cybersecurity Unit' <www.justice.gov/criminal-ccips/cybersecurity-unit> accessed 23 August 2018.

[536] Good Night Lamp <http://goodnightlamp.com/> accessed 24 August 2018.

Vignette	Vignette example	Actual example/source
J5	Internet-connected oven	Jenn-Air Connected Wall Oven[537]
J5	Connected smoke alarms	Nest Protect Smoke Alarm[538]
J7	Breathalyser lock	Smart Start Interlocks[539]
J9	Internet-connected hairbrush	Kerastase Hair Coach powered by Withings and L'Oreal[540]
J9 + J13 + J14	Smart hub/digital personal assistant (Max)	Amazon's Alexa-controlled Echo Speaker[541]
J10	Interactive billboard	Smart interactive billboard device[542]
J11	Internet-connected doll (Ella)	My Friend Cayla[543]

[537] Jenn-Air <https://jennair.com/connect> accessed 25 August 2018.

[538] Nest <https://nest.com/smoke-co-alarm/overview/>accessed 25 August 2018.

[539] Smart Start Interlocks <www.smartstartinterlocks.com.au/products.html> accessed 23 August 2018.

[540] Brian Heater, 'Here's a Smart Hairbrush with a Built-In Microphone from Withings and L'Oreal' (*Techcrunch*, 3 January 2017) <https://techcrunch.com/2017/01/03/withings-brush/> accessed 15 November 2017.

[541] Amazon, 'Echo and Alexa' <www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4/ref=sr_1_cc_1?s=aps&ie=UTF8&qid=1534996023&sr=1-1-catcorr&keywords=echo+speaker+alexa> accessed 23 August 2018. See also Kiran K Edara, 'Keyword Determinations from Voice Data' (*Google Patents*, 23 September 2011) <https://patents.google.com/patent/US8798995B1> accessed 1 July 2018.

[542] Agency for Science Technology and Research Singapore, 'Smart Interactive Billboard Device' (US Patent Application US20050021393A1) <https://patents.google.com/patent/US20050021393A1/en> accessed 5 September 2018. See also Tim Johnson, 'Smart Billboards Are Checking You Out – And Making Judgments' *The Seattle Times* (Seattle, 26 September 2017) <www.seattletimes.com/business/smart-billboards-are-checking-you-out-and-making-judgments/> accessed 24 August 2018.

[543] Genesis Toys, 'My Friend Cayla' <www.myfriendcayla.com/> accessed 5 September 2018. This doll is pre-programmed with phrases that advertise Disney products: Jeff John Roberts, 'Privacy Groups Claim These Popular Dolls Spy on Kids' (*Fortune*, 8 December 2016) <http://fortune.com/2016/12/08/my-friend-cayla-doll/> accessed 20 November 2017.

Vignette	Vignette example	Actual example/source
K1	General purpose health monitoring device	DXTER™[544]
K2	Smart medication bottle	Vitality GlowCap[545]
K3	Smart watch	Apple Watch Series 3[546]

3.3 Lessons learned

Early drafts of the Vignettes written prior to 2017 were much more 'speculative' than what is now contained in this chapter. Later on in the drafting process, the more speculative elements of the Vignettes were removed. This was done to avoid the problems of 'over-speculation' identified in **section 2.1** of this chapter,[547] such as the potential distraction away from real problems, and an undesirable focus on technologically specific solutions.

However, some material originally written as 'speculative' has been included in the final version of the Vignettes contained in this chapter. This occurred as 'real-life' examples of originally speculative material began to emerge during the course of doctoral candidature, and real technological developments overtook the initial 'fiction' of some of the Vignettes and made it into fact. This underscored the value of the attributes and interaction framework to inform the research and the Vignettes, as the drafting of the early Vignettes was based on this framework.

[544] Basil Leaf Technologies, 'DXTER™: A New Kind of Consumer Medical Device' <www.basilleaftech.com/dxter/> accessed 31 December 2018. The technology is still under development. See Best, 'Building the Tricorder: The Race to Create a Real-Life Star Trek Medical Scanner' (n 162).

[545] Jen Hodson, 'NantHealth's Vitality Mobile App Now Available on Apple and Android Devices' (Press Release, 26 October 2017) <https://nanthealth.com/nanthealths-vitality-mobile-app-now-available-apple-android-devices/> accessed 24 August 2018.

[546] Apple (n 161) accessed 25 August 2018.

[547] Bennett Moses, 'Regulating Beyond Nanotechnology' (n 487) 43.

Two examples of this follow. First, in **Vignette J9**, Max's capacity to listen in on and react to conversations was originally speculative. However, in late March 2018 news broke of a 'voice-sniffing' patent filed by Amazon, which allows Amazon's real-life equivalent of Max to do exactly that (although the company denies that it uses the functionality).[548] Additionally, in February 2019, controversy arose when Google revealed that its Nest Secure home security systems contained a microphone capable of picking up voice commands and other sounds, a feature missing from the specifications of the product since its launch in 2017.[549] Further media reports as to private conversations being inadvertently sent as voice files to third parties have confirmed both the power, and the dangers, of such technology.[550] Second, the possibility of the use of eObjects as a tool for domestic abuse (discussed in **sections 3.1.1** and **3.1.5** of **Chapter 5**) was originally part of 'speculative' vignettes. However, in April 2017 the author of this dissertation presented at a workshop on eObjects and security issues.[551] At this workshop a representative of a women's services organisation reported[552] that the organisation had already seen a number of incidences of domestic violence facilitated by eObjects. These Australian experiences are not unique, as

[548] Sapna Maheshwari, 'Hey, Alexa, What Can You Hear? And What Will You Do With It?' *The New York Times* (New York, 31 March 2018) <www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html> accessed 4 April 2018.

[549] Sydney Fussell, 'The Microphones That May Be Hidden in Your Home' *The Atlantic* (23 February 2019) <www.theatlantic.com/technology/archive/2019/02/googles-home-security-devices-had-hidden-microphones/583387/> accessed 26 February 2019.

[550] Hamza Shaban, 'An Amazon Echo Recorded a Family's Conversation, Then Sent it to a Random Person in Their Contacts, Report Says' *Washington Post* (Washington, 24 May 2018) <www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says> accessed 30 May 2018.

[551] UNSW-ACCAN Smart Home Internet of Things Security workshop, UNSW Kensington, 20 April 2017.

[552] The workshop was held under the Chatham House Rule, which prohibits the disclosure of 'the identity … or the affiliation of the speaker(s), [or] that of any other participant': Chatham House (The Royal Institute of International Affairs), 'Chatham House Rule' <www.chathamhouse.org/chatham-house-rule> accessed 9 September 2018.

indicated in a report of technology-enabled US domestic violence by the *New York Times* in July 2018.[553]

4 CONCLUDING REMARKS

This chapter has provided a series of Vignettes to illustrate the impact on consumers' lives of eObjects and the systems in which they participate. The Vignettes' primary function in this dissertation is to illustrate in a reader-friendly form the attributes and interactions framework developed in **Chapter 2.** More specifically, these Vignettes will be used in **Chapter 5** to illustrate the *challenges* that consumers will face in their everyday lives in relation to eObjects and the systems in which they participate. Some of the Vignettes are also further discussed in **Chapter 6** to illustrate examples of how the *law* may apply to sociotechnical change brought about by eObjects, particularly in relation to certain forms of marketing enabled by eObjects.

[553] Nellie Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' *The New York Times* (New York, 23 June 2018) <www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 25 June 2018.

Chapter 5 – Challenges for consumers[554]

[554] This chapter reproduces substantial parts of a journal article published during the course of doctoral study: Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (n 95).

1 AIMS OF CHAPTER

> We are stuck with technology when what we really want is just stuff that works.[555]

Most of the scholarly literature on eObjects to date has not generally concerned itself with consumer protection. Rather, it more narrowly concentrates on the privacy, data protection and security implications of the ready availability of a potentially vast store of data about individuals, their lives, and their preferences. Much of the early literature focussed on the inadequacy of existing privacy laws to protect individuals.[556] From the commencement of research on this dissertation in 2013 until recently, only a small amount of literature raised misgivings about the effect on consumers

[555] Douglas Adams, *The Salmon of Doubt: Hitchhiking the Galaxy One Last Time* (Harmony Books 2002) 115.

[556] For example, Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88); Thierer, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation' (n 88); Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (n 144); Ridge, 'What Happens When Everything Becomes Connected: The Impact on Privacy when Technology Becomes Pervasive' (n 88).

and their contracts with suppliers, and these discussions were preliminary and brief.[557]

However, as discussed in **Chapter** 1, from late 2015 consumer[558] and non-profit[559] groups, as well as some scholars[560] and practitioners,[561] began to raise concerns that consumers may face particular challenges in relation to the sale, purchase and use of eObjects. These challenges arise not only in relation to the attributes of eObjects but in the marketing activities and contractual arrangements used by providers of goods, services and infrastructure relating to eObjects.

Section 3 of **Chapter 3** discussed the importance of identifying the goals or purposes of the law of consumer contracts in order to uncover legal problems. **Section 4** of **Chapter 3** proceeded to identify the relevant goals, called the **Consumer Goals** for the purposes of this dissertation. This chapter uses this recent literature and the technical research framework contained in **Chapter 2** to identify the challenges that consumers may face where the outcomes have the potential to conflict with the Consumer Goals. The Vignettes developed in **Chapter 4** are also used in this chapter to assist

[557] Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (n 61); Peppet, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (n 62); Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88); Kim, 'Two Alternate Visions of Contract Law in 2025' (n 89); Kang and Cuff, 'Pervasive Computing: Embedding the Public Sphere' (n 89); Cherry, 'A Eulogy for the EULA' (n 89); Calo, 'Digital Market Manipulation' (n 42).

[558] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63); Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63).

[559] Rose, Eldridge and Chapin, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (n 63).

[560] Early draft and pre-publication versions of the following began appearing on SSRN in late 2015 and early 2016: Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42); Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93); Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94); Millard, Hon and Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (n 87).

[561] For example, Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing?' (n 103); Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (n 103).

readers to understand in detail the nature of sociotechnical change brought about by eObjects and the systems in which they participate. This chapter does not attempt to uncover *actual* legal problems, but rather the *potential* for them in particular challenges for consumers.

Most eObjects do not contain radically new technology; rather, they result from a combination of incremental improvements, or the use of current technologies in new contexts. Therefore, the effect of single attributes or interactions is often not particularly significant. However, particular combinations of attributes and/or interactions give rise to significant innovations (based not only on concepts of 'newness' but also on changes of scale or purpose). As discussed in **section 2.2.4** of **Chapter 3**, this dissertation suggests that legal problems relating to sociotechnical change are most likely to be found in innovations. However, it is important to note that just because an innovation is identified, and a challenge for consumers arises out of this innovation, this does not automatically mean that a corresponding legal problem exists (see discussion of regulatory disconnection and legal problems in **section 2.2.1.2** of **Chapter 3**). Existing laws may already apply to any harm to consumers arising out of the innovation.

Section 2 of this chapter details the importance of understanding the complex nature of eObjects and the systems in which they participate when identifying challenges of consumers. It also sets out an informal classification scheme for the challenges identified in this chapter. Note that some of these challenges are not entirely 'new'; nor do they appear only with eObjects. As discussed in **section 2.2.4** of **Chapter 3**, Koops proposed that a change in scale of use of an existing technology could produce its own problems, in addition to 'radically new' technologies. **Section 3** of this chapter discusses in detail both new challenges and challenges that are significantly exacerbated by the advent of eObjects,[562] because of the scale of their use,

[562] This distinction between new and exacerbated challenges is well illustrated in Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 26.

the particular combination of attributes and/or interactions of eObjects, or for other reasons. Also briefly mentioned in **section 3** are other challenges that consumers of eObjects have 'in common' with consumers of other types of consumer products, but where the existence of eObjects does not bring about a new challenge or significant exacerbation of an existing challenge.

2 IDENTIFYING CHALLENGES FOR CONSUMERS

2.1 eObjects, systems and services

When identifying the challenges for consumers, it is important to consider the underlying complex and interrelated nature of eObjects and the systems in which they participate. All eObjects comprise a physical object or living thing, hardware in the form of a computer processor and software. Many eObjects are also components of 'product–service packages',[563] where services are provided alongside the eObject as essential or optional elements of the functionality provided. Additionally, as discussed in **section 4.2.2** of **Chapter 2**, many eObjects may be nested within a larger eObject, or form elements of a larger, distributed system. Challenges for consumers arising out of eObjects may relate to a single eObject, or to the whole or some elements of the 'ecosystem'[564] in which the eObject participates including:

- pairs or groups of eObjects (particularly when a remote controller is used, whether a dedicated device or a smartphone);
- a larger, distributed system comprising multiple eObjects and other elements; and/or
- the software and/or services provided in relation to the eObject and the system in which it participates.

[563] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 141.

[564] The term 'ecosystem' was adopted from Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) and Millard, Hon and Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (n 87).

Any or all of these elements of hardware, software, object or service may be supplied by different entities. For example, a recent case study[565] of the smart thermostat sold by Nest analysed an eObject ecosystem and the myriad different parties who provide some part of it including:

- manufacturer;
- cloud providers (for data storage, synchronisation, communication and redundancy);
- analytics;
- payment processing;
- advertising services;
- 'Safety Rewards';[566]
- energy partners (providing processing power);
- website developer;
- app store;
- embedded software developers;
- ISPs;
- network operators;
- ecommerce platforms;
- resellers;
- retailers;
- wholesale distributors; and
- installers.

Other actors may also be relevant when assessing challenges to consumers, such as designers, component manufacturers, assemblers, importers, distributors, those providing software integration services and testers. The authors of the case study above use the phrase 'supply chain' to describe these actors. This term, while commonly used, is misleading in these circumstances as it implies serial, linear connections. Such linear connections will often not apply to particular ecosystems incorporating

[565] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 5–9.

[566] The researchers could not identify what this service actually constituted from the documents provided.

eObjects. This dissertation uses the alternative phrase 'provider network' to indicate more accurately the nature of the connections between the different actors involved in the provision of an eObject to market and beyond.[567] This dissertation also uses the term 'Provider' to indicate an entity in the provider network.

2.2 Classification of challenges

This chapter sets out aspects of eObjects and the systems in which they participate that might pose challenges for consumers where outcomes conflict with the goals of consumer protection law. These challenges cannot be categorised by individual attribute or interaction as, due to the nature of eObjects, the challenges are often caused by a combination of various attributes and/or interactions. Therefore, they have been clustered into broader groups of characteristics as listed below. These groups are not proposed as a formal classification scheme, but rather a collection of similar issues for ease of discussion in this dissertation, and other types of groupings are possible. These broader groups are not mutually exclusive. Particular challenges may fit in more than one group, and relevant goals may also apply to more than one group. Note that the references to 'Core' attributes in the following discussion refer to those attributes referred to in **section 4.2.2** of **Chapter 2**.

[567] The concept of a 'network' rather than a 'chain' has been discussed in other contexts, although different terms have been used. See, for example, discussions of: 'virtual organisation' in Kai Riemer and Nadine Vehring, 'Virtual or Vague? A Literature Review Exposing Conceptual Differences in Defining Virtual Organizations in IS Research' (21st Bled eConference: eCollaboration: Overcoming Boundaries Through Multi-Channel Interaction, Bled, Slovenia, June 15–18); 'business ecosystem' in Marco Iansiti and Roy Levien, 'Strategy as Ecology' (2004) 82 Harvard Business Review 68; and 'meta-organization' in Ranjay Gulati, Phanish Puranam and Michael Tushman, 'Meta-Organization Design: Rethinking Design in Interorganizational and Community Contexts' (2012) 33 Strategic Management Journal 571.

This dissertation argues that consumers face significant challenges due to the following features of eObjects and the systems in which they participate. eObjects and the systems in which they participate may:

1) be *imperfect* (see **section 3.1** of this chapter)
   Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability[568] to ensure eObjects operate reliably. For example, many are vulnerable to remote security breaches, and where an eObject (or something that it is connected to) has active capacity, it can cause physical or mental harm remotely, as well as economic loss. These sorts of losses may also occur from volatile access to resources, inaccuracy of data, and autonomous decision-making by eObjects. How Providers ultimately manage, or fail to manage, these risks may also be a challenge for consumers.

2) be *controlled* and *modified* remotely by Providers (see **section 3.2** of this chapter)
   In many eObjects the programmable computers they contain may be remotely accessed. As a result, their functionality, content and interoperability with other devices and other features can be controlled or modified remotely without the intervention, consent or even knowledge of the owner/user. In many circumstances, modifications (and certain types of control) cannot be put into effect by the consumer, but only by a Provider. (Note that control by third parties other than a Provider is also important, but this issue is discussed in **section 3.1** of this chapter.)

3) be used to *manipulate* or *impede consumer choice* (see **section 3.3** of this chapter)
   Some attributes in eObjects can put up barriers to a consumer's freedom to contract. For example, an eObject with significant autonomy may make decisions that cannot be overridden (or not easily so) or are not

[568] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 135–36.

even obvious to the user due to the invisibility of the device or the decision-making process.

4) have a significant *post-supply value* to Providers (see **section 3.4** of this chapter)
   The use pattern of eObjects can mean that significant post-supply value can be exploited: for example, in reuse or sale of the data collected by the eObject, or in the long-term recoupment of contractual premiums for licences or other services provided. Where End User Licence Agreements (**EULAs**) or Acceptable Use Policies (**AUPs**) are in place, the value for Providers may be found where the contractual conditions affect the use of the software or digital content in ways that the relevant intellectual property legislation does not.

5) be *complex* (see **section 3.5** of this chapter)
   Most eObjects are inherently complex, due to their **interactions** with living things, the physical world, other eObjects and/or other computing devices and systems. Many eObjects are hybrids of object, software, hardware and service/s, as functionality often requires associated services to be acquired, such as access to cloud data handling facilities and a website interface. Even more complexity arises when eObjects' embedment in larger systems is considered. As illustrated in **section 2.1** of this chapter, many entities can be involved in providing the hardware, software, object and services involved. Therefore, complexity arises not only from the eObjects themselves, but the nature of the contractual arrangements that are required to keep such eObjects running.

3 THE CHALLENGES

In the next section, references to Attributes and Interactions are to the core and other attributes and interactions of eObjects set out in **sections 4.2.2**, **4.2.3** and **4.2.4** of **Chapter 2**.

3.1 Imperfection

In 2013, Townsend contended that due to the nature of eObjects, smart cities are 'buggy, brittle and bugged'.[569] The first two parts of this description are applicable to many eObjects, and to many systems in which eObjects participate, whether as a part of a smart city or otherwise. This is particularly the case with eObjects marketed to consumers. Suppliers with low profit margins and modest experience in computing products may have little incentive or capability[570] to ensure that eObjects are particularly reliable in their operation.

Sometimes, choosing low-quality, discardable (and therefore cheap) individual eObjects may be a sensible choice for eObjects ecosystems. For example, in swarm systems (such as drones for surveillance[571] or agricultural applications[572]), component-level failures can often be dealt with at a system level[573] reducing the impact of the failure. However, even in swarm systems, unreliable control mechanisms of **mobile** eObjects or eObjects with significant **active capacity** can be problematic if they allow swarm components to escape control without shutting down.[574]

Particular challenges for consumers arising from the imperfection of eObjects' design and manufacture are set out below.

[569] Anthony M Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (WW Norton & Co 2013) ch 9.

[570] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 135.

[571] Roger Clarke, 'Understanding the Drone Epidemic' (2014) 30 Computer Law and Security Review 230, 235.

[572] ECHORD++ (European Coordination Hub for Open Robotics Development), 'MARS: Mobile Agricultural Robot Swarms' <http://echord.eu/mars/> accessed 23 February 2018.

[573] Liguo Qin, Xiao He and DH Zhou, 'A Survey of Fault Diagnosis for Swarm Systems' (2014) 2 Systems Science & Control Engineering 13.

[574] Clarke, 'Understanding the Drone Epidemic' (n 571) 235.

3.1.1 Security problems

Attributes and Interactions: **Vulnerability, mobility, active capacity**

Consumer Goal/s: **SafeFit**

Vulnerability is an important attribute of many consumer eObjects and ecosystems. In the early days of eObjects, Satyanarayanan argued that eObjects are more prone to physical interference than conventional computing devices.[575] This is especially so for mobile hardware, such as smartphones or wearable electronic devices, which is easily stolen or damaged.[576] More recently, a deluge of reports indicates that some eObjects may well be more prone than conventional connected computers not just to physical interference but also to remote attacks. Security researchers have recently proven the ease of remote attacks on consumer devices such as: fitness trackers;[577] medical devices such as insulin pumps, heart defibrillators and CT scanners;[578] domestic appliances such as Internet-connected

[575] Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (n 285) 1.

[576] For example, the Fitbit Flex wristband (commercially available) which contains sensors which tracks physical activity and sleep patterns, and then syncs with smartphones or conventional computers to create a data profile. See Fitbit (n 308).

[577] For example, Fitbit (n 308). See Rahman, Carbunar and Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (n 11); Barcena, Wueest and Lau, *How Safe is Your Quantified Self?* (n 11).

[578] Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (n 569) 269. Other healthcare eObjects with identified security concerns include drug infusion pumps, X-ray systems and blood refrigeration units: see Kim Zetter, 'Medical Devices That Are Vulnerable to Life-Threatening Hacks' (*Wired,* 24 November 2015) <www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x> accessed 3 May 2016.

kettles[579] and 'smart' TVs;[580] baby monitors;[581] location trackers;[582] children's toys;[583] guns;[584] and larger devices such as cars.[585] The prevalence of security vulnerabilities is such that security researchers and others have begun to keep lists of known security issues with eObjects and related systems.[586] In January 2018, the Australian Therapeutic Goods Administration expressed concern about the identification by non-profit research organisation ECRI Institute of 'ransomware and other cybersecurity threats' as its highest ranking health technology hazard for 2018.[587] The existence of ransomware

[579] Catalin Cimpanu, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks across London' (*Softpedia,* 20 October 2015) <http://news.softpedia.com/news/insecure-internet-connected-kettles-help-researchers-crack-wifi-networks-across-london-494895.shtml> accessed 12 November 2015.

[580] Consumer Reports, 'Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds' (*Consumer Reports*, 7 February 2018) <www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/> accessed 8 August 2018.

[581] Kashmir Hill, 'Watch Out, New Parents – Internet-Connected Baby Monitors Are Easy to Hack' (Splinter, 2 September 2015) <https://splinternews.com/watch-out-new-parents-internet-connected-baby-monitors-1793850489/> accessed 24 April 2019.

[582] Lorenzo Franceschi-Bicchierai, 'A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them' (*Motherboard*, 3 February 2016) <https://motherboard.vice.com/en_us/article/bmvnzz/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them > accessed 24 April 2019.

[583] Security Ledger, 'Update: Hello Barbie Fails Another Security Test' (n 12); ForbrukerRadet (Norwegian Consumer Council), 'Connected Toys Violate European Consumer Law' <www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/> accessed 9 July 2018.

[584] Andy Greenberg and Kim Zetter, 'How the Internet of Things Got Hacked' (*Wired*, 28 December 2015) <www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/>.

[585] Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' (*Wired,* 21 July 2015) <www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> accessed 1 September 2015; Stephen Checkoway and others, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' (Proceedings of USENIX Security 2011, August 2011); Nick Bilton, 'Disruptions: As New Targets for Hackers, Your Car and Your House' *The New York Times* (New York, 11 August 2013) <http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0> accessed 2 February 2017.

[586] Code Curmudgeon, 'IoT Hall-of-Shame' <https://codecurmudgeon.com/wp/iot-hall-shame/> accessed 9 July 2018.

[587] Therapeutic Goods Administration, 'ECRI Lists Ransomware as 2018 Top Hazard' (2018) 6 Medical Devices Safety Update 2. See also Timothy Webb and Sumer Dayal, 'Medical Devices and the IoT: Regulatory Perspectives on Cybersecurity Risks in

provides one incentive to malicious actors to threaten the exploitation of vulnerability in eObjects.

Increased risk of remote attack is substantially due to the existence of particular security vulnerabilities in the eObjects themselves and the systems in which they participate, such as:

- insecure network services, interfaces, software and/or firmware;
- lack of encryption;
- insufficient authentication and authorisation and/or security configurability;
- the way personal data is stored; and
- the lack of physical safeguards.[588]

These vulnerabilities can leave the devices open to remote attacks, which can include the remote operation of the eObject without the permission of the local user ('hacking') and/or the delivery of malicious software ('malware'). Consequences of these types of attacks include:

- disclosure or modification of sensitive data;
- attacks against other eObjects or conventional computers; and/or
- physical harm to or destruction of the eObject, surrounding objects and/or people.[589]

For example, in September 2016, the website of security journalist Brian Krebs experienced a distributed denial of service (**DDoS**) attack delivered

Health Care' (2018) Internet Law Bulletin 138; Heather Landi, 'Report: Ransomware Attacks on IoT Medical Devices Will Likely Increase' (*Healthcare Informatics*, 29 November 2016) <www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware> accessed 13 January 2017.

[588] This is a consolidated list adapted from Open Web Application Security Project (OWASP), 'OWASP Internet of Things Project' (2014) <www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29> accessed 12 January 2017.

[589] This is a consolidated list adapted from Cloud Security Alliance, 'Security Guidance for Early Adopters of the Internet of Things (IoT)' (Mobile Working Group, Peer Reviewed Document, April 2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 8 July 2017.

primarily through eObjects.[590] Significant increases in reported DDoS attacks during 2017 have also been attributed in part to the growth in numbers of eObjects.[591]

Why such security vulnerabilities are so common in eObjects and the systems in which they participate has been attributed to:

- the inexperience of (and possible lack of interest by) consumer goods manufacturers in security issues (as compared to specialist IT manufacturers);[592]
- the small size of some devices rendering them unable to support the processing power and energy demands required for strong security measures such as encryption;[593]
- many devices having been designed (for reasons of cost and fitness for purpose) in such a way that hardware and software access, management, and/or monitoring are difficult or impossible.[594] For example, some devices are not designed to accommodate software updates, making security patches unworkable;[595]

[590] Brian Krebs, 'KrebsOnSecurity Hit With Record DDoS' (*KrebsOnSecurity,* 21 September 2016) <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/> accessed 24 October 2016.

[591] Corero, 'Corero DDoS Trends Report Q2–Q3 2017' (2017) <http://info.corero.com/rs/258-JCF-941/images/2017-q2q3-ddos-trends-report.pdf> accessed 10 July 2018.

[592] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 94.

[593] Ibid.

[594] Katie Boeckl and others, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (National Institute of Standards and Technology Internal Report 8228 (Draft), September 2018) 7–8. Problems can arise from '[l]ack of management features … [l]ack of interfaces … [d]ifficulties with management at scale … [a w]ide variety of software to manage … [d]iffering lifespan expectations … [u]nserviceable hardware … [l]ack of inventory capabilities … [and h]eterogenous ownership'.

[595] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 135–36. Also see Bruce Schneier, 'The Internet of Things is Wildly Insecure – And Often Unpatchable' (*Wired*, 1 June 2014) <www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/> accessed 17 December 2015.

- the sheer number of attack surfaces available to an attacker when many eObjects are connected to one organisation's network;[596] and
- the fact that common post-market cybersecurity controls used for conventional IT (such as firewalls, anti-malware servers or network-based intrusion prevention systems) may be ineffective for eObjects, as eObjects may use alternative protocols or communicate point-to-point rather than through a monitored infrastructure network.[597]

Security problems with consumer eObjects may also be exacerbated when security features are furnished by a Provider that disappears from the provider network and is not replaced, resulting in the absence of both expertise and security updates. This might happen when a Provider is subjected to external administration, or management makes a business decision to stop supporting the relevant product (which may be motivated by attempts to minimise the threat of liability for existing defects that cannot be remedied without substantial investment).

Security implications are particularly acute with intimately personal eObjects and their potential harm to one person, but there are many other contexts in which security issues manifest themselves.

One of the key consequences of technological developments related to eObjects is the re-emergence of physical spaces and places as an important concept in information technology.[598] The physical location of an embedded smart device forms an essential part of its nature, and is inextricably linked

[596] Rose, Eldridge and Chapin, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (n 63) 21; American Bar Association Section of Science & Technology Law, *Submission to the National Telecommunications and Information Administration, US Dept of Commerce, in response to Docket No. 160331306-6306-01: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things* (2016) 11.

[597] Boeckl and others, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (n 594) 9.

[598] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) ch 5; Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (n 144) chs 1, 4.

to its use by humans.[599] Similarly, the ability of a mobile device to move quickly and easily in space between physical locations without losing functionality profoundly affects the nature of its use.

One of the most obvious implications of the physicality of devices and systems in eObjects is their vulnerability to the security concerns outlined above, particularly in the example of security exploits of motor vehicles. In the last five years, security researchers have successfully managed to exploit flaws in some cars' Internet-connected internal systems in order to wirelessly control the cars' locks, brakes, steering and transmission (as well as tracking their geographic location).[600] Within the world of eObjects, an innovation that may hold significant danger arises from the interaction between the eObject attributes of **vulnerability** and **mobility.** For example, in **Vignette J6**, Jessica's loss of control of her smart car and subsequent car accident may have been deliberately caused by a person – such as her ex-partner, Steve – executing a remote attack. An attack might be undertaken for the specific reason of causing physical harm, but even attacks undertaken for other purposes, such as surveillance and tracking, may have unintended consequences. Perpetrators do not even need to be themselves particularly skilled in cybersecurity exploits. Malware kits and development expertise can now be readily and anonymously purchased online in the form of 'hacking as a service' (**HaaS**).[601] One of the HaaS platforms, 'Hackers' List' in 2018 openly advertised its services to be used for 'check[ing] on a cheating spouse'.[602]

---

[599] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 109.

[600] Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' (n 585); Checkoway and others, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' (n 585); Bilton, 'Disruptions: As New Targets for Hackers, Your Car and Your House' (n 585).

[601] Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data* (Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, 15 March 2018) 9.

[602] Hackers' List, 'Hacker for Hire FAQ' <https://hackerslist.com/FAQ.html> accessed 7 July 2018. Access to the site was attempted again on 25 April 2019 but it had been removed. However, in 2019 a similar site posted customer testimonials

A desktop computer is a large and heavy object, and hackers have not been generally able to pick one up and throw it across a room. However, in the world of eObjects, malicious third parties may have the power to remotely control a one-and-a-half tonne piece of metal travelling at 100km/hour and use it (or a fleet of them) to injure people and property.

The much-vaunted 'smart home' potentially brings with it similar practical problems, although **mobility** is not usually the attribute interacting with **vulnerability** here. Rather it is **active capacity**, being the ability of eObjects to interact with the physical world. The fire in Jessica's apartment (**Vignette J5**) is a good example of loss which may occur as a result of the interaction between the vulnerability and active capacity attributes of eObjects. Again, the damage may not have resulted from a deliberate attempt to cause a fire, but happenstance, error and unintended consequences can result in harmful security incidents, even without an intention to cause a specific type of harm.

Other more direct harms may be possible due to **active capacity** of an eObject. Security researchers have successfully exploited a vulnerability in an Internet-connected toilet, allowing it to remotely squirt water.[603] But more sinister mischief is possible. Security flaws in a connected sniper rifle raise the possibility of remote-controlled murder or grievous bodily harm. Security researchers have developed proofs of concept for a security attack to shut down smart light bulbs across an entire city,[604] and to use eObject botnets[605] of devices such as air conditioners and heaters to 'launch large-

regarding hacked university grades, partner's mobile phones, and credit reports. See HackersList, 'How it Works' <https://www.hackerslist.co/how-it-works/> accessed 24 April 2019.

[603] Jasper Hamill, 'Hackers Take Control of a Toilet Using Bog-Standard Computer Skills' *The Mirror* (London, 10 February 2016) <www.mirror.co.uk/tech/hackers-take-control-toilet-using-7342662> accessed 5 September 2018.

[604] Danielle Correa, 'IoT Lightbulb Worm Takes Over All Smart Lights until Entire City Is Infected' (*SC Magazine*, 10 November 2016) <www.scmagazineuk.com/iot-lightbulb-worm-takes-smart-lights-until-entire-city-infected/article/1475933> accessed 14 December 2016.

[605] A botnet can be defined as 'a collection of remotely controlled and compromised computers known as bots … that installs software (typically malicious) on the bots'

scale coordinated attacks on the power grid'.[606] Such measures are ripe for exploitation by criminal networks and terrorists, with potential to cause both physical and economic loss. Soltan and others also raise the possibility that exploits could be undertaken in order to benefit individual suppliers within an energy market, for example by forcing increased demand for power which in turn would raise prices for reserve power generators.[607]

The adult sex toy market appears to be subject to similar risks, with the potential for disturbing consequences. The first eObject vibrator was released commercially in 2015, and since then security vulnerabilities have been identified in at least two connected vibrators on the market.[608] These vibrators are designed to be remotely controlled, for example via a Bluetooth connection to a smartphone,[609] and the risk of non-consensual access to these devices due to poor security raises the possibility of remote sexual assault.

The Consumer Goal of **SafeFit** aims to ensure that goods and services are safe and fit for the purposes for which they were sold. Where security exploits are readily available and the eObject has the capacity to have an effect in the physical world, this obviously compromises the physical safety of consumers. Even a security exploit that simply shuts down an eObject without other physical consequences will compromise the second limb of the **SafeFit** Consumer Goal, as an eObject that cannot be used is not fit for purpose.

computer and performs acts, nearly always criminal, using the innocent bot computer': Alana Maurushat, 'Zombie Botnets' (2010) 7 Scripted 2.

[606] Saleh Soltan, Prateek Mittal and H Vincent Poor, 'BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid' (Proceedings of the 27th USENIX Security Symposium, 15–17 August 2018, Baltimore) 15.

[607] Ibid 16.

[608] Kate Lawrence, 'Should the Internet of Vibrating Things Be Worried?' (*Readwrite*, 13 October 2016) <http://readwrite.com/2016/10/13/should-the-internet-of-vibrating-things-be-worried-dl1/ > accessed 6 December 2016.

[609] For example, We-Vibe <https://we-vibe.com/> accessed 1 January 2018.

3.1.2 Volatility of resources

Attributes and Interactions: **Volatility, active capacity, visibility**

Consumer Goal/s: **SafeFit**

Increased volatility of eObjects, and the systems in which they participate, may have harmful side effects. Satyanarayanan was among the first to outline what he considered the major 'constraints of mobility', which differentiated first mobile and then pervasive computing from other forms of distributed computing.[610] Satyanarayanan claimed that smart devices will always be 'resource-poor' in relation to conventional desktop computing, in particular in relation to processing and network speed, memory and storage, due to considerations of 'weight, power, size and ergonomics'.[611]

Coulouris, writing 15 years later, essentially agreed with Satyanarayanan as to these constraints and their continuing relevance despite advances in technology, but conflated them within his concept of 'volatility', a condition in which 'the set of users, devices and software components in any given environment is liable to change frequently'.[612] **Volatility** constraints in eObjects manifest themselves in the different types of connections, energy sources and processing power utilised by smart devices. In particular, connectivity of devices using wireless networks (whether the device is mobile or embedded) is usually more variable in relation to bandwidth, latency and reliability. There may also be associated indirect restraints based on common business models. For example, mobile data charges in Australia are often more expensive for consumers than home fixed-wireless charges.

[610] Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (n 285); Satyanarayanan, 'Pervasive Computing: Vision and Challenges' (n 190). Satyanarayanan's papers are still widely quoted by modern computer scientists: for example, Adelstein and others, *Fundamentals of Mobile and Pervasive Computing* (n 20) 5; Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192); Coulouris and others, *Distributed Systems: Concepts and Design* (n 192).

[611] Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (n 285) 1.

[612] Coulouris and others, *Distributed Systems: Concepts and Design* (n 192) 817ff.

However, while the constraints of mobility are real and continuing, they do not necessarily operate in the same way for all smart devices. Some eObjects, such as mobile phones, have access to large amounts of processing power, memory and storage. Others, such as low-power sensors, draw from alternative energy sources to access what is effectively unlimited power for their lifetime.[613] However, for many eObjects, volatility constraints will drive a design that will not be optimal on all fronts. For example, many eObjects still need to be designed to minimise power consumption, with corresponding negative effects on processing power and speed. Some security methods commonly used in conventional computing, such as crypto-processing, are notably detrimentally affected by volatility constraints.[614] Current alternatives developed to overcome these constraints, such as lightweight cryptography methods, are known to trade off performance against resource drain, with the result that security may be compromised compared to conventional systems.[615]

The challenges for consumers in this respect are in relation to their protection against failures of eObjects due to resource constraints, such as when a power source is drained or when connectivity is lost. Those using eObjects with **active capacity**, particularly those with low **visibility**, have the highest risk of loss. Failure, with the risk of serious physical and personal loss, due to resource constraints may not be immediately obvious to the user. This risk is most obvious in industries such as healthcare, where the failure of devices such as wirelessly controlled insulin pumps and pacemakers can cause serious harm or even death. For example, Kylie's pacemaker (**Vignette K1**) is currently of an age at which battery failure is common, but

[613] For example, solar-powered calculators, or piezoelectric energy harvesters, which convert kinetic energy such as vibrations into electrical energy. See for example, Piezo.com (a division of Mide Technology) range at Mide Technology, 'Piezoelectric Energy Harvesters' <https://piezo.com/collections/piezoelectric-energy-harvesters?_=pf&pf_t_quantity=Quantity__1> accessed 23 February 2019.

[614] William J Buchanan, Shancang Li and Rameez Asif, *Lightweight Cryptography Methods* (Taylor & Francis 2017) 187.

[615] Ibid 188. Also see generally Fadele Ayotunde Alaba and others, 'Internet of Things Security: A Survey' (2017) 88 Journal of Network and Computer Applications 10.

replacement brings its own risk of infection.[616] However, volatility problems are not just important in implanted devices. For example, as illustrated in **Vignette J6**, volatility in a GPS-based service may make Kitt liable to getting lost while in automated mode.

Therefore, for similar reasons to those set out in **section 3.1.1** of this chapter, volatility may make eObjects either unsafe, not fit for purpose, or both, compromising the Consumer Goal of **SafeFit**. It is not 'new' that consumer products suffer from resource constraints, especially when compared with similar products produced for business, but consumer problems may be exacerbated in two areas: the introduction of new failure points for consumer devices, such as failure of connectivity; and the hidden nature of some of the failures, such as discussed above in relation to healthcare devices.

3.1.3 Accuracy

Attributes and Interactions: **Core, autonomy, active capacity**
Consumer Goal/s: **SafeFit, Disadvantage**

All eObjects have the capacity to **collect, handle and communicate data**. Data may be, or become, inaccurate during the eObject's performance of any of these three processes. Sensors can be misled by physical phenomena; algorithms can be wrong; data records can be corrupted. Additionally, accuracy problems can arise from imperfection in the sensors themselves, such as their design, build and calibration, or due to damage to them or normal wear over time. The collection and processing of data may also be detrimentally affected by the environmental conditions.[617] In the eObjects

[616] Anna Hodgekiss, 'Pacemaker Safety Alert: Thousands of Patients "At Risk of Serious Infection Because Battery Life Isn't Long Enough"' (*Daily Mail Australia*, 5 February 2016) <www.dailymail.co.uk/health/article-3431734/Pacemaker-safety-alert-Thousands-patients-risk-infection-battery-life-isn-t-long-enough.html> accessed 4 November 2016.

[617] Roger Clarke, 'Quality Factors in Big Data and Big Data Analytics' (19 December 2014) <www.rogerclarke.com/EC/BDQF.html#DQF> accessed 23 October 2018.

context, questions have already been raised about the accuracy of accelerometers[618] and sleep trackers.[619]

Consumers (and for that matter Providers) who rely on such data are at the risk of physical or other harm if such data is inaccurate.[620] For example, if the notification generated on the smart container regarding Kylie's pill-taking schedule in **Vignette K2** is incorrect, Kylie's reliance on it may lead to a harmful overdose. Similarly, if Fahim's continuous glucose monitor (**Vignette F1**) reports incorrect results, its **active capacity** may lead to a dangerous dose of insulin or a failure to act by the device.

Similar problems with inaccuracy were identified in a pre-eObjects context. For example, from 1985 to 1987, two people died and others were injured when computerised radiotherapy machines of a particular model used in US and Canadian hospitals administered massive overdoses of radiation to patients, partially due to a failsafe counter being erroneously set to zero in inappropriate circumstances.[621] In Saudi Arabia in 1991, a Patriot missile defence battery failed to fire due to an incorrect time calculation. The failure to fire prevented an attempt to interdict an Iraqi Scud which subsequently killed 28 people and injured over 100.[622]

The challenge of accuracy is exacerbated in eObjects (as opposed to non-connected devices) for at least two reasons: (1) scale; and (2) physical distancing of human override, monitoring or control. In relation to scale, health eObjects provide a good example. Estimates of growth in the global

[618] KL Dannecker and others, 'A Comparison of Energy Expenditure Estimation of Several Physical Activity Monitors' (2013) 45 Medicine and Science in Sports and Exercise 2105.

[619] HE Montgomery-Downs, SP Insana and JA Bond, 'Movement Toward a Novel Activity Monitoring Device' (2012) 16 Sleep Breath 913.

[620] Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87).

[621] NG Leveson and CS Turner, 'An Investigation of the Therac-25 Accidents' (1993) 26 Computer 18, 34.

[622] Douglas N Arnold, 'The Patriot Missile Failure' <www-users.math.umn.edu/~arnold/disasters/patriot.html> accessed 7 July 2018.

healthcare eObjects market vary significantly, but even conservative appraisals predict a market of well in excess of USD100 billion by 2020.[623] The connectedness of medical eObjects to internetworks will mean that human controllers or fail-safe systems may be a long way from the eObject, and any decisions they make will also be subject to inaccurate data that is fed from the device. Additionally, many kinds of eObjects (particularly mass-produced, low-cost devices) may be difficult or impossible to maintain due to the lack of features allowing testing, recalibration and replacement parts.

Inaccuracy of data may render an eObject unsafe or dysfunctional, which conflicts with the Consumer Goal of **SafeFit**. Those who rely on eObjects for their medical care may well be vulnerable and/or disadvantaged, and therefore detrimental outcomes for them may well also conflict with the Consumer Goal of minimising **Disadvantage**.

3.1.4 Autonomy

Attributes and Interactions: **Autonomy**
Consumer Goal/s: **SafeFit, Redress, Choice**

eObjects that have some **autonomous** action and/or decision-making capability (either alone or as part of the system in which they participate) can also cause problems for consumers. Decision-making algorithms can be programmed to result in outcomes that are not desired by the user. The algorithms themselves are usually opaque to consumers, either due to a deliberate attempt to protect proprietary information or simply because they require sophisticated technical knowledge to be understood. Additionally, as machine learning becomes more sophisticated, eObjects may develop

[623] Grand View Research, 'Internet of Things in Healthcare Market Size, Industry Report 2019–2025' (November 2018) <www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market> accessed 23 February 2019; Markets and Markets, 'IoT Healthcare Market Worth 163.24 Billion USD by 2020' <www.marketsandmarkets.com/PressReleases/iot-healthcare.asp> accessed 7 July 2018; TJ McCue, '$117 Billion Market for Internet of Things in Healthcare by 2020' (*Forbes*, 22 April 2015) <www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#26c66b5f2471>.

emergent features that could not have been foreseen even by those who have access to, and the capacity to understand, the algorithms.[624] This may be because the original algorithm developers do not have access to the same data as the eObject, or the assumptions of the implicit model underlying the processing embody assumptions that are not updated when the environment changes.

Consequently, an **autonomous** eObject with **active capacity** could cause physical harm without any intention or intervention by the user or a third party. For example, it is certainly not far-fetched to postulate that Fahim's robot cleaner (**Vignette F6**) could make decisions about speed and direction that cause it to run over Medusa's tail, or cause furniture to topple over. This is even more likely when a new variable is introduced, such as a new pet or a new chair. The possibility of consumer products causing physical harm is not new, but **autonomous** decision-making capabilities may make the harm more difficult to predict.

An eObject's decision-making capabilities *could* also cause economic harm, for example in the context of eObjects that sell themselves or other things. Economic harm is not inevitable: many transactions instituted in this manner will not be significantly different from those facilitated by vending machines or similar methods of automatic distribution. For example, Jessica's smart coffee machine (**Vignette J2**) may be set by Jessica to automatically order more coffee pods when it is in danger of running out, and if her instructions are followed, this should not cause new challenges for her. However, some situations where the eObject exercises autonomous decision-making capacity may cause unwanted outcomes.[625] For example, what if Jessica presses her Wulwurths AutoBuy button just once (**Vignette J2**), but a decision is made by the eObject (for example due to a

[624] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) Big Data & Society 1, 3–5; Will Knight, 'The Dark Secret at the Heart of AI' (2017) 120 MIT Technology Review 54, 56.

[625] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 4.

'buy in bulk' cost-minimisation strategy) that results in an order of 1000 cartons of washing detergent instead of one?

There are already multiple examples of problems with automated buying and selling using conventional (non-eObjects) computing techniques. For example, the use of automated comparative pricing algorithms by two Amazon book merchants led to the pricing of an out-of-print textbook on the genetics of flies at a high of USD23 698 655.93.[626] Although this is an extreme example, less extreme automated nudging of higher prices may be harmful to consumers. Automated high-frequency trading software was arguably a key factor in the May 2010 US 'Flash Crash',[627] which saw the Dow Jones Industrial Average lose 9% of its value in less than 30 minutes, a drop which was then unprecedented.[628]

In cases where the decision-making by the eObject cannot be predicted, interesting questions may arise.[629] What if the reordering facility on Jessica's coffee machine (**Vignette J2**) contained machine learning capabilities that assessed the coffee consumption across the months she has been in the apartment? And what if the order was based, not on a bug or malfunction, but on the eObject's assessment of likely preferences in this scenario? Jessica until recently shared the apartment with Steve; he may have been a coffee addict with a penchant for expensive single-origin blends, while she is happy with the occasional cup of budget coffee. The coffee machine's assessment of Flat No 7's preferences based on its previous learning may then be significantly flawed. In contrast to the physical harms outlined above, these types of economic harm are not unique to eObjects; rather, they are

[626] Michael Eisen, 'Amazon's $23,698,655.93 Book about Flies' (*it is NOT junk: a blog about genomes, DNA, evolution, open science, baseball and other important things,* 22 April 2011) <www.michaeleisen.org/blog/?p=358> accessed 3 January 2017.

[627] Andrei Kirilenko and others, 'The Flash Crash: High-Frequency Trading in an Electronic Market' (2017) 72 Journal of Finance 967.

[628] US Commodity Futures Trading Commission and US Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues* (30 September 2010) 1.

[629] Millard, Hon and Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (n 87) 287.

additional examples of harms that have already arisen in conventional computing settings.

The most obvious Consumer Goal that may be offended in this case is that of **SafeFit,** as products may not provide consumers with the expected outcome. However, the Consumer Goals of both **Choice** and **Redress** may also be compromised, as this situation raises the fundamental question of liability for the actions of a machine. For example, who will be liable for an unfavourable and unwanted contract entered into by a machine, which was not predictable by the user (or indeed the programmer) of such a machine?

3.1.5 Management of risk by Providers

Attributes and Interactions: **All** in **sections 3.1.1** to **3.1.4** of this chapter

Consumer Goal/s: **SafeFit, Redress, Information**

As discussed above, the imperfection of eObjects leads to significant risks of harm to consumers. Risk management is further complicated by the nature of many eObjects as product–service packages, or merely one component within a complex ecosystem, and further where there are multiple players in the provider network. Therefore, the question of how a Provider intends to manage these risks is an important concern for a consumer, and is discussed in this section. The ability of a consumer to properly understand the nature of the risks in order to make an informed choice is also an important concern, particularly considering the complexity of eObjects. This challenge is discussed in **section 3.5.1** of this chapter.

There are three areas where consumers will face significant challenges in relation to how Providers intend to manage risk:

1) Proactive management of risk: what are each Provider's obligations in relation to monitoring and updating of software?[630]
2) When things go wrong: who will be responsible for fixing problems with the eObject?[631]

[630] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 194–95.
[631] Ibid 195–96.

3) What limitations will Providers attempt to place on their obligations regarding risk management?

Considering the risks outlined in **sections 3.1.1–3.1.4** of this chapter, these are important things for the consumer to know before they enter into a contract. This can be illustrated by examining **Vignette J4**.

When examining the house-servicing contract/s relevant to the smart lock, Jessica should be concerned with the answers to a number of questions. In addition to understanding the general position as to which Providers have obligations under the contract, and the specific nature and limits of those obligations, Jessica should also be considering these specific questions:

- What monitoring of security risks are Providers doing and how quickly will they know that something is wrong?
- When and how will the consumer be notified if there is a vulnerability?
- Exactly which Provider is responsible for supplying security patches, when will these be available, who is responsible for installing them, and in what timeframe?
- If urgent repair is needed, and either the provisions for repair or the agreed timeframe is inadequate, what rights does the consumer have to bring in an unrelated third party to have the lock made secure? Any locksmith can replace or lock a conventional house lock, but will administrative passwords or proprietary knowledge of other security measures be required to fix or replace a lock in a smart home?
- What limits does the contract place on Provider liability for damage caused due to the failure of the smart lock? Does it cover repair, damage to property and personal harm?
- What are the obligations of the Provider if other parts of the smart home system cause a disruption to the operation of the smart lock?
- What happens if Smart Lock Pty Ltd is in external administration?

Consumer judgment on the adequacy of answers to these questions may well be essential to a choice between competing products. As with other products and services, there is an inevitable tension between a seller's obligation to notify consumers, and a consumer's obligation to inform themselves, about risks relating to eObjects. However, many consumers will not be technically

sophisticated enough, or have enough time, or be in a sufficiently attentive state of mind, to think of and ask the right questions, or to understand the answers, or to consider all possible future uses. So, in cases where information is not readily available, is unintelligible to a reasonable consumer, or is uncertain, efficient competition may not be fostered, leading to a conflict with the Consumer Goal of **Information**. This is discussed further in **section 3.5.1** of this chapter.

Risk allocation issues are relevant to almost every supply and service contract, and are not specific to eObjects. However, there are some areas where eObjects will exacerbate these issues, or introduce new issues. For example, in any contract, if Providers are allowed to drastically limit their liability without some form of core responsibility, this will come into conflict with the Consumer Goal of **SafeFit.** Attempts to limit supplier liability are already commonplace: but problems of risk allocation become particularly pertinent when a Provider's ability to remotely modify an eObject after the original supply to the consumer means that an eObject originally fit for purpose later becomes unfit due to the Provider modification. This is discussed further in **section 3.2** of this chapter.

Additionally, problems with information, safety and quality may not be the only problems. In **Vignette J4**, Jessica's ability to manage her smart home is likely to be affected by the fact that she herself has no contract with members of the provider network for the smart lock or indeed any of the smart home services. This is despite the fact that the actions (or inaction) of Providers can cause significant continuing damage to Jessica. For example, she may not be able to prevent Steve entering the apartment if she cannot change the administrator password on the smart lock. This danger is not merely theoretical. Reports are now emerging of eObjects in connected homes being used as tools of domestic abuse.[632] Although family violence is not a new problem, the advent of eObjects, particularly those embedded in people's homes, presents new opportunities for its execution. Often, no

[632] Bowles, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' (n 553).

security exploit is even required, as the perpetrators of the abuse are often the contracting parties and hold all the passwords. If Jessica herself was not a contracting party, she will have no contractual right to have the administrator password changed. In any event, Jessica's lack of a legal right may be unimportant if Smart Locks Pty Ltd has been wound up or is no longer trading. Similar problems may arise for new owners if Jessica sells her apartment.

These problems could conflict with the Consumer Goal of **Redress,** as Jessica may not have any legal rights to compel any party to rectify her situation or give her compensation for any loss.

3.2 Provider control

Attributes and Interactions: **Core, Dependency**

Consumer Goal/s: **SafeFit, Fairness, Redress**

The capacity of eObjects for **data handling and data communication**, and in some cases their **dependency** on remote services and infrastructure, exposes consumers to a number of challenges. eObjects and the systems in which they participate may be designed so that Providers can control or modify all or part of the eObject, the data held within it, the behaviour of the eObject, and/or the services supplied along with the eObject. Consumers may not have the means to prevent Providers exercising their powers to control or modify, and may not even realise that these powers exist, or when and how they have been exercised. This potential for change in the eObject is distinctly innovative, at least at the scale now possible. Most physical consumer goods are generally only subject to change imposed by time and environment (for example, wear and tear) or initiated by the customer who actively and directly transfers possession (for example, repair or replacement).

Note that this section deals solely with remote control and disablement by members of the provider network. **Section 3.1.1** of this chapter dealt with control and disablement by unauthorised 'rogues': that is, third parties exploiting security vulnerabilities. Note, however, that while Providers may

be authorised by the terms of supply to control and/or disable devices and systems, this is not always the case. The authorisation may be contingent on one or more pre-conditions being satisfied. *Unauthorised* access by a Provider remains possible.

In many cases it is also feasible for one or more Providers to:

- disable temporarily or permanently all or part of an eObject's functionality;
- program the eObject to work differently or produce a different user experience by modifications to the eObject or its associated services;
- remove or modify digital content stored on the eObject; and/or
- prevent changes by the user to the eObject, for example the modification of personalisation features or the removal of data.[633]

A connected eObject can be remotely disabled, for example where a purchase instalment or a related service fee has not been paid. Starter interrupt devices (like the one installed in Fahim's car in **Vignette F7**) allow lenders or their agents to remotely disable a vehicle using their mobile phones. Lenders may well be contractually entitled to this type of disablement when owners are late on car repayments. Such devices had been installed in approximately 2 million cars in the US by late 2014.[634] The ability to disable an eObject remotely gives considerable powers to Providers that are either not available or not practical to enforce for consumer goods that are not eObjects. And these rights, and the ability to enforce them anytime, anywhere, can lead to new circumstances of harm to consumers. For example, a 2014 *New York Times* article reported that the remote triggering of a starter interrupt device in a car prevented a mother from taking her asthmatic child to the hospital. It was also reported that another woman was

[633] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 200–02.

[634] Michael Corkery and Jessica Silver-Greenberg, 'Miss a Payment? Good Luck Moving That Car' *The New York Times* (New York, 24 September 2014) <http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_php=true&_type=blogs&ref=business&_r=0> accessed 2 February 2017.

forced off the road when her car powered down, allegedly due to the use of an interrupt device by her lender.[635]

Other forms of disablement are less direct, and much less likely to be subject to overt consumer agreement or understanding. Revolv's smart home hub hardware and application was shut down less than two years after it was issued. This occurred after Nest (a subsidiary in the Alphabet/Google corporate group) acquired the company but refused to support the product any longer.[636] In December 2016, the smartwatch manufacturer Pebble announced to its customers that: it was closing down its business; it had sold its intellectual property rights to Fitbit; warranty support for all Pebble products was immediately discontinued; and the company announced 'Pebble functionality or service quality may be reduced in the future.'[637] Disablement does not only occur when there is a change of ownership. The smart home hubs Sony Dash and Harmony Link were shut down by the companies that released them, although not without backlash from consumers.[638]

Reduced or discontinued functionality of eObjects can also come about in other ways. Examples include where a Provider issues an upgrade to firmware or other software that makes the hardware completely unusable[639]

[635] Ibid.

[636] Woodrow Hartzog and Evan Selinger, 'The Internet of Heirlooms and Disposable Things' (2016) 17 North Carolina Journal of Law & Technology 581, 584.

[637] Pebble, 'Pebble's Next Step' (7 December 2016) <https://blog.getpebble.com/2016/12/07/fitbit/#more-1032> accessed 11 July 2018. As of 24 April 2019, this site had been shut down. The author of this dissertation acknowledges a personal interest in this: she owned a Pebble watch for two months and was just about to return it under warranty due to a fault when the announcement was made.

[638] Sony, 'Support' (13 July 2017) <https://esupport.sony.com/US/p/news-item.pl?news_id=519> accessed 23 September 2018; Brian Barrett, 'After Backlash, Logitech Will Upgrade All Harmony Link Owners for Free' (*Wired,* 9 November 2017) <www.wired.com/story/logitech-giving-harmony-link-owners-a-free-harmony-hub/> accessed 11 July 2018.

[639] Adam Boult, Cristina Criddle and Cara McGoogan, 'Apple's New iOS 10 Update Causes Major 'Bricking' Problems for iPhone and iPad Users' *The Telegraph* (London, 15 September 2016) <www.telegraph.co.uk/technology/2016/09/13/ios-10-launch-live-how-to-upgrade-to-apples-new-software-and-wha/> accessed 30 October 2016. Also

or causes the eObject's data handling capabilities to run extremely slowly. Two lawsuits are known to have been filed in the US relating to allegations that Apple's software updates to iPhones have slowed down performance.[640] Or a service provider may go into liquidation or simply decide to discontinue a service, such as cloud data storage and processing. This may make the eObject much less valuable or even worthless to the consumer if there are no viable service substitutes available, either due to the state of the market or to technical interoperability problems.

In some cases, these types of disablement may be unintended by the Provider. In other cases they may be deliberate, such as in the case of planned obsolescence, or where a Provider is acquired by a competitor (such as when Fitbit acquired Pebble). In any event, a consumer may have no choice but to buy a device with upgraded hardware, or to pay a premium price for an upgraded service. Jessica may be facing this situation with her smart lock (**Vignette J4**) if the service provider indeed cannot be found. In order to protect herself she may need to install a whole new smart lock system.

Digital content resident on or accessed through eObjects may well be blocked in order to protect the rights of intellectual property holders, such as when there is no record of a user holding a licence to that content.[641] However, control mechanisms by Providers have been used to deny access to content in circumstances where the consumer has not been involved in a breach of contract or any wrongdoing. In 2009, Amazon remotely deleted copies of George Orwell's novel *1984* from the Kindle e-book readers of

see user comments in Samuel Gibbs, 'iOS9 Making Your iPhone Slow? You're Not Alone' *The Guardian* (Sydney, 24 September 2015) <www.theguardian.com/technology/2015/sep/24/iphone-slow-ios-9-update-iphone-4s-iphone-5-iphone-5s> accessed 12 January 2017.

[640] See Mikey Campbell, 'Lawsuit Seeks More than $5M from Apple for Slowing Older iPhones with iOS 9 Upgrade' (*appleinsider,* 29 December 2015) <http://appleinsider.com/articles/15/12/29/lawsuit-seeks-more-than-5m-from-apple-for-allegedly-slowing-older-iphones-with-ios-9-upgrade> accessed 30 October 2016.

[641] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 201–02.

customers who had legitimately paid for the book. This was done when Amazon discovered that the third party who loaded the book into Amazon's digital store did not have the right to do so. Interestingly, Amazon did not appear to have included an express term in its contract with consumers to allow for this type of remote deletion.[642] Jessica's *MacGyver* files (**Vignette J3**), if locally held, may well be subject to the same sort of treatment, or her file-downloading and/or streaming capabilities may be blocked.

The potential for direct and remote enforcement of Provider rights, or alleged rights, is a new challenge for consumers. Remote disablement based on intellectual property rights, or a right to repossess for failure to pay a debt, may be considered as merely a reflection of what could have been imposed by means of a court order. However, the newness of the challenge for consumers subsists in the immediacy and inflexibility of such Provider reactions. The safeguard of engagement in a formal dispute resolution process, overseen by a neutral party, the court, will no longer apply to protect the consumer until well after detriment has occurred.[643] The ease and low cost of remote disablement can be expected to lead to a far greater incidence of its use, and in far less serious cases, than the past practice of seeking court orders imposing similar remedies. There is a real risk that disablement will be treated as something much more routine by businesses than the initiation of litigation and this may result in its less careful application and consequent erroneous action. Many consumers will not have the knowledge or resources to mount an action against inappropriate disablement, with the consequence that the problem could become entrenched.

[642] Brad Stone, 'Amazon Erases Orwell Books from Kindle' *The New York Times* (New York, 18 July 2009) <www.nytimes.com/2009/07/18/technology/companies/18amazon.html> accessed 18 May 2016.

[643] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 35–36.

The situations outlined above indicate a clear conflict with the Consumer Goal of **SafeFit,** and in some cases, **Redress**. It is worthwhile noting that in these situations, the eObject as originally supplied to the user may well have been fit for purpose. It may be only afterwards that, by a deliberate or inadvertent act by a Provider, the case becomes otherwise. However, there may be conflict with another goal. The ability of Providers to act in this way, often supported by non-negotiable contractual terms explicitly granting the right to such modifications, could also conflict with the Consumer Goal of **Fairness**.

3.3 Consumer choice

3.3.1 Digital consumer manipulation

Attributes and Interactions: **Core, geo-locatability, adaptability, mobility, prevalence, use pattern**

Consumer Goal/s: **Disadvantage, Fairness, Choice**

> We left the Eisner and started up Broadway, the Everly Readers in the sidewalk reading the Everly Strips in our shoes, the building-mounted mini-screens at eye level showing images reflective of the Personal Preferences we'd stated on our monthly Everly Preference Worksheets, the numerous Cybec Sudden Emergent Screens outthrusting or down-thrusting inches from our faces, and in addition I could very clearly hear the sound-only messages being beamed to me and me alone via various Kakio Aural Focussers, such as one that shouted out to me between Forty-second and Forty-third, 'Mr. Petrillo, you chose Burger King eight times last fiscal year but only two times thus far this fiscal year, please do not forsake us now, there is a store one block north!,' in the voice of Broadway star Elaine Weston ...[644]

Saunders' 2002 short story, 'My Flamboyant Grandson', illustrates a potential future for consumers due to the emergence of eObjects. As the use of

[644] George Saunders, 'My Flamboyant Grandson' *The New Yorker* (28 January 2002) 78.

eObjects becomes more widespread, this increases the likelihood that a greater quantity of data – and data which is more intimate and personalised in quality – can and will be collected and processed. The rise of the data broker industry[645] also allows data to be easily shared amongst corporate entities and contributes to significant diffusion of that data. The inferences that can be derived from all of this data can be used for purposes that *some* consumers might perceive to be beneficial: for example, better targeting of advertising.[646] However, many uses are far less beneficial.

There is growing concern by scholars,[647] practitioners,[648] think tanks[649] and industry commentators[650] that the increase in electronic marketing and transactions may grant marketers a significantly increased capacity to discover consumer preferences, and use data and behavioural research to exploit the biases, emotions and vulnerabilities of consumers.[651] For example,

[645] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014).

[646] Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy: Emerging Issues in data Collection, Use and Sharing* (Consumer Policy Research Centre, July 2018) 35.

[647] Calo, 'Digital Market Manipulation' (n 42); Kim, 'Two Alternate Visions of Contract Law in 2025' (n 89); Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42); Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42); Anthony Nadler and Lee McGuigan, 'An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing' (2018) 35 Critical Studies in Media Communication 151; Damian Clifford, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making – A True Path to the Dark Side?' (CiTiP Working Paper 31/2017, KU Leuven Centre for IT & IP Law, submitted 15 September 2017) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037425> accessed 30 April 2018.

[648] Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (n 103) 7.

[649] Wolfie Christl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (A Report by Cracked Labs, Vienna, June 2017); Nguyen and Solomon, *Consumer data and the digital economy: emerging issues in data collection, use and sharing* (n 646) 23–24.

[650] For example, Yael Grauer, 'Dark Patterns Are Designed to Trick You (And They're All Over the Web)' (*arsTECHNICA*, 28 July 2016) <http://arstechnica.com/security/2016/07/dark-patterns-are-designed-to-trick-you-and-theyre-all-over-the-web/> accessed 1 May 2018.

[651] Calo, 'Digital Market Manipulation' (n 42) 995ff; Kim, 'Two Alternate Visions of Contract Law in 2025' (n 89) 312; Helberger, 'Profiling and Targeting Consumers in

advertisers (as well as search engines) may: filter the information made available to consumers; target consumers at the time when their willpower is lowest; and/or craft their advertisements to act upon known purchasing triggers of particular individuals, such as feelings of guilt or obligation or concerns about missing out or a desire to emulate friends or celebrities.

The US scholar Ryan Calo dubbed this practice 'digital market manipulation'.[652] This term is rooted in an earlier concept, 'market manipulation', which was coined by Hanson and Kysar in the late 1990s.[653] The term became widely cited in the subsequent US literature.[654] This literature explains how commercial entities use techniques to exploit consumers' cognitive limitations and biases to sell them products and services.

However, Calo, Hanson and Kylar's terminology may create confusion in an Australian context, as its use of the word 'market' is likely to produce different associations for Australian readers. First, section 1041A of the Corporations Act 2001 (Cth) established an offence of 'market manipulation'. It prohibits conduct that creates or maintains an artificial price for a financial product. Second, the use of 'market' may produce confusion as to whether the conduct referred to must affect conditions at a market level, rather than individual consumers. A significant whole-of-market effect may occur where the conduct is prevalent and successful, but disbenefits for consumers can arise even when the conduct does not have a significant effect on the overall market.[655] This dissertation does not examine whether

---

the Internet of Things: A New Challenge for Consumer Law' (n 42) 140–61; Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 1ff; Halliday and Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (n 103) 7.

[652] Calo, 'Digital Market Manipulation' (n 42) 995.

[653] Jon D Hanson and Douglas A Kysar, 'Taking Behavioralism Seriously: Some Evidence of Market Manipulation' (1999) 112 Harvard Law Review 1420; Jon D Hanson and Douglas A Kysar, 'Taking Behavioralism Seriously: The Problem of Market Manipulation' (1999) 74 New York University Law Review 630.

[654] The two relevant papers have been cited over 200 times each. See Calo, 'Digital Market Manipulation' (n 42) fn 29.

[655] Roger Clarke, 'Risks Inherent in the Digital Surveillance Economy: A Research Agenda' (2019) 34 Journal of Information Technology.

particular conduct has a whole-of-market effect and the resulting adequacy of Australia's competition laws. Rather, the effect of conduct on individual consumers will be examined. Hence, the term 'digital consumer manipulation' is used in preference to 'digital market manipulation'. The term 'consumer' has already been defined in **section 3.4** of **Chapter 1**, and the 'digital' in the term refers to digital technologies defined in **section 3.5** of **Chapter 1**. This dissertation proposes the following definition of 'digital consumer manipulation':

> *the use of personalised consumer data collected, processed and/or disseminated by digital technologies, combined with insights from behavioural research, to exploit consumers' cognitive biases, emotions and/or individual vulnerabilities for commercial benefit.*

The commercial benefit to be gained from such techniques might be the direct purchase of products or services, the handing over of additional data, charging inflated prices for goods or services, or even merely creating an increased liking for a brand that is then recommended in some way to other consumers.

An examination of the core and other attributes present in eObjects and related systems reveals several attributes that can enhance opportunities for digital consumer manipulation, and therefore exacerbate the challenge for consumers that such conduct poses. This is particularly the case when viewed in conjunction with the development of sophisticated data processing techniques. The capacity of all eObjects to **collect** and **communicate** data assists marketers in building customer profiles and in targeting their marketing campaigns. Marketers can also leverage other attributes of eObjects, such as **mobility**, to improve their chances of success. Even where the eObject is embedded rather than mobile, the mobility of *people* interacting with the embedded eObject can increase the amount and variety of data that is collected, especially considering the increasing **prevalence** of eObjects.

Within the traditional model of distributed information technologies, the place where a desktop is physically located has been irrelevant in most contexts,[656] and difficult to determine accurately. However, now many eObjects are mobile, and their **use pattern** is more likely to be 'personal': that is, intimately associated with an individual. This greatly enhances both the value of the **geo-locational** functionality, and the utility of the data gathered and communicated by the eObject. The **use pattern** of many eObjects is often limited to one or a few individuals, and the eObject may also be **geo-locatable**, **addressable** and/or **identifiable**. A subsequent ability to personalise data records improves the usefulness of the data gathered. The utility of the data is also increased by another attribute of eObjects, **adaptability** (also known as 'context awareness'). An adaptable eObject can identify in real time some part of its user's context: that is, who the user is, where she is, the environment through which she is moving, her habits and her preferences. The eObject, or the system in which it participates, can reconfigure and adapt itself accordingly.[657]

This means that increased deployment of eObjects and related systems will provide opportunities for a greater volume of more intimate and personalised data to be collected and used. This data can be used to build customer profiles and inform behavioural research and advertising delivery. The eObjects themselves can also be used to target and deliver advertising messages, as well as provide a conveniently swift purchase mechanism (reducing the time available for consumers to change their minds). Therefore, this section (and the in-depth doctrinal analysis in **Chapter 6**) discusses the concept of 'digital consumer manipulation' enabled, in whole or in part, by eObjects.

[656] There is at least one notable exception to this: 'geoblocking' (the practice of limiting access to content, particularly TV programs and movies, on the Internet based on your geographic location): see for example, Karl Schaffarczyk, 'Explainer: What is Geoblocking?' (*The Conversation*, 17 April 2013) <http://theconversation.com/explainer-what-is-geoblocking-13057> accessed 3 May 2016.

[657] Aarts and Roovers, 'IC Design Challenges for Ambient Intelligence' (n 245) 2–3.

Recent international legal developments may also encourage the use of technologies capable of collecting consumer data and using it to target advertising towards consumers. Article 17 (previously Article 13) of the proposed new EU Directive on copyright[658] requires information-society service providers to take measures to block unlicensed copyright material, including through the 'use of effective content recognition technologies'. Current content recognition technologies, such as Audible Magic, Vobile and INA, commonly include analytical techniques devised in order to deliver information about 'what viewers search for, how they view their favourite shows or movies, listen to favourite music … [and] how images are used'.[659] Romero-Mareno argues that Article 17 will 'serve … as the legal basis for social network platforms and rightsholders to use … users' analytics for targeted display advertising'.[660]

Digital consumer manipulation already exists in some form, mostly emanating from conventional ecommerce (although smartphones are often involved). For example, Netflix and Amazon have developed procedures based upon customers' preferences, profiles or past usage that enable these companies to recommend tailored products and services. Pandora, the Internet radio service, displays political ads based on its consumers' music preferences. Shazam does the same for consumer goods such as cars.[661]

There are various examples of digital consumer manipulation involving eObjects ecosystems that have been imagined. **Section 3.3.1** of this chapter

[658] Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market COM(2016)593. The Directive passed the European Parliament on 26 March 2019, but requires formal endorsement by the Council of the European Union.

[659] European Commission, *Commission Staff Working Document Impact Assessment on the modernisation of EU copyright rules SWD(2016) 301* (2016) 165.

[660] Felipe Romero-Moreno, '"Notice and Staydown" and Social Media: Amending Article 13 of the Proposed Directive on Copyright' (2018) 32 International Review of Law, Computers & Technology 18 (page number of article published online 29 May 2018).

[661] Natasha Singer, 'Listen to Pandora, and It Listens Back' *New York Times* (New York, 4 January 2014) <www.nytimes.com/2014/01/05/technology/pandora-mines-users-data-to-better-target-ads.html> accessed 21 October 2017.

began with an extract from a prescient 2002 *New Yorker* story. Another example was provided in 1996 by legal and architecture scholars Kang and Cuff who postulated the development of a 'networked mall'.[662] This is a mixed real/virtual shopping centre created by the use of existing and (at the time) speculative technologies involving eObjects and related systems. Kang and Cuff conjectured that Providers in a networked mall might attempt digital consumer manipulation in many different ways. For example, music in a particular part of the store might change in response to the person entering, health monitor readings detecting a temperature might trigger a mobile telephone advertisement for paracetamol or the local medical centre, or a 'sudden up-tick [of heart rate] near lingerie might suggest a rated R feature at the gigaplex'.[663]

Although both Kang and Cuff's idea of a networked mall and Saunders' networked and media-saturated streetscape were speculative at the time, over a decade of technological development has seen the realisation of some of their ideas. For example, by 2014, the data from mobile phone sensors had been claimed to enable inferences about mood, personality, stress levels, gender, marital and job status, age, level of disease, mental health issues, sleep and physical movement.[664] For example, in 2013 researchers were able to extract from smartphones audio, GPS and accelerometer data, call numbers, call duration, ratio of incoming to outgoing calls, changes in phone contacts, phone numbers and email addresses and battery usage, and analyse this data to predict stress levels in the smartphone user.[665]

[662] Kang and Cuff, 'Pervasive Computing: Embedding the Public Sphere' (n 245) 121–45.

[663] Ibid 126.

[664] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 115–16; Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (n 67) 15.

[665] Amir Muaremi, Bert Arnrich and Gerhard Tröster, 'Towards Measuring Stress with Smartphones and Wearable Devices during Workday and Sleep' (2013) 3 BioNanoScience 172.

eObjects have also been developed specifically for use as enterprise marketing devices. 'Beacon' implementation systems, such as Apple's iBeacon, use indoor positioning devices and systems with small, low-power sensors[666] that are capable of tracking when a smartphone enters a particular physical space. Such systems marry precise geo-location and contextual data (for example, retail products within close proximity, purchase history and preferences, time of day) in order to target personalised marketing communications to the most likely buyers. For example, a shopper who has signed up to the service (by downloading an app)[667] may be located by a beacon as he enters a clothing store. A general discount voucher may then be sent to his phone. Additionally, systems with more sophisticated algorithms and programming might access his marketing profile, see that he is a keen shoe shopper, and generate a *personalised* discount voucher to the shopper for certain designer shoes in the aisle nearest to him. Audio beacons are also being used, although they have attracted litigation in the US due to allegations of recording conversations without permission, in breach of the so-called Federal 'Wiretap Act'.[668]

Although the use of beacon technology is not yet widespread, by 2018 it was being used or piloted by retail, fast food, sporting, airline and real estate services, and by pharmacies and other business enterprises both in

[666] iBeacon uses the Bluetooth Low Energy communications standard, but other beacon technologies use both Bluetooth and Wi-Fi (for example, Motorola Solutions and Datzing).

[667] Such as Beaconnected (n 524).

[668] Electronic Communications Privacy Act 18 USC § 2510. In 2016, Signal360 was allegedly using both Bluetooth beacons and audio beacons. An audio beacon system includes speakers mapped to a location and emitting a unique audio signal, and a corresponding mobile phone application that turns on the phone's microphone in order to 'listen' to the audio signals from the beacons. In 2016 a class action was filed in California, alleging that the application recorded the audio of private conversations of a basketball team's fans without permission. See *Satchell v Sonic Notify Inc*, No 4:16-cv-04961 (ND Cal). A similar action was filed in October 2016, this time relating to the audio recording of fans of a football team. See *Rackemann v Lisnr Inc*, No 2:16-cv-01573 (WD Pa).

Australia[669] and overseas[670] with varying levels of success. Interest in similar corporate tracking technologies appears to be growing. For example, in October 2018, a member of Chemist Warehouse's IT architecture team announced that the pharmacy business was 'considering' installing thousands of sensors to track foot traffic within its stores and where consumers 'dwell in particular areas [and] … pick up products and look at them'.[671]

Returning to the Vignettes, the timing of the doughnut discount offer on Fahim's phone (**Vignettes F2** and **F4**) may not be a coincidence. His proximity to the doughnut store, the time of day and its likely correlation to low levels of willpower, and his past consumer behaviour, together point to an optimised marketing opportunity.

The accuracy of consumer profiles and opportunities for behavioural targeting may be assisted by the use of additional technologies, such as cross-device tracking technologies (known as 'XDT'). XDT allow tracking of a consumer across multiple devices, for example by tracking a consumer's television viewing by means of software installed on their smartphone.[672] Companies such as Google, Domino's and Nestlé have been using services provided by XDT companies such as SilverPush, Signal360 and Audible

[669] Woolworths Ltd (major supermarket chain), Homepass (real estate services). See Localz, 'Localz' <https://localz.com/customer-stories/> accessed 9 September 2018.

[670] For example, Macy's, McDonald's, Major League Baseball, Walgreens, Virgin Atlantic, Japan Airlines, American Airlines: Trips Reddy, '15 Companies from Airports to Retail Already Using Beacon Technology' <www.umbel.com/blog/mobile/15-companies-using-beacon-technology/> accessed 10 November 2014; James Wood, 'iBeacon: The Future of Content Marketing?' *B2B Marketing* < https://www.b2bmarketing.net/en/resources/blog/ibeacon-future-content-marketing> accessed 17 February 2014. Also John Lewis (department store): Localz, 'Localz' (n 669).

[671] Ry Crozier, 'Chemist Warehouse Could Create an Internet of Medicine' (*iTnews*, 18 October 2018) <www.itnews.com.au/news/chemist-warehouse-could-create-an-internet-of-medicine-514130> accessed 18 October 2018.

[672] See for example, Federal Trade Commission, *Cross-Device Tracking: An FTC Staff Report* (January 2017); Justin Brookman and others, 'Cross-Device Tracking: Measurement and Disclosures' (2017) 2 Proceedings on Privacy Enhancing Technologies 133.

Magic, although not without controversy.[673] In 2016, the US Federal Trade Commission issued warning letters to Android application developers who used XDT technologies from SilverPush that could track television viewing habits even when the application in question was not in use.[674]

These types of marketing systems rely on eObjects with access to personalised customer profile data, with the potential to be programmed in response to behavioural research on how consumers make decisions to buy goods or services. They may also respond to the personal preferences and likely behaviour of the actual consumer targeted by the beacon at any one time. Despite the lack of the 'human touch' in selling, this can provide distinct marketing advantages. An average human shop assistant, faced with a new customer, is unlikely to have the same knowledge of their personal preferences. Nor are they likely to have access to the aggregated knowledge of purchasing patterns or cognitive biases[675] capable of being collected and contained within an eObject and associated systems. The persuasive powers of a human person may not even be an advantage. Some psychological research has indicated that people can react the same way to social persuasion (such as flattery or kindness) by a computer as they do to real people.[676] So a real-life implementation of Saunders' 'Kakio Aural Focusser' (introduced at the beginning of this section) pleading abandonment issues in order to convince the narrator to buy Burger King may meet with some success. Digital personal assistants, or 'helpers' in the home, such as

[673] John Leydon, 'Anti-Ultrasound Tech Aims to Foil the Dog-Whistle Marketeers' (*The Register*, 4 November 2016) <www.theregister.co.uk/2016/11/04/marketing_privacy/> accessed 30 January 2018.

[674] Federal Trade Commission, 'FTC Issues Warning Letters to App Developers Using "Silverpush" Code' (Press Release, 17 March 2016) <www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code> accessed 4 March 2018.

[675] For a good summary of cognitive biases that might affect consumer decision-making, see M Neil Browne and others, 'Protecting Consumers from Themselves: Consumer Law and the Vulnerable Consumer' (2014) 63 Drake Law Review 157, 182–90.

[676] Calo, 'Digital Market Manipulation' (n 42) 1040; BJ Fogg, *Persuasive Technology: Using Computers to Change What We Think and Do* (Morgan Kaufmann Publishers 2003) 103–05.

Amazon's Alexa, and Alphabet's Google Assistant, provide contemporary examples of the potential that these types of devices have for both data collection and marketing delivery. For example, Amazon's Alexa and associated cloud services record and store voice requests for music, audio books, podcasts, web searches about 'various subjects' including health conditions and politics, and real-time information such as news, weather and traffic conditions. They also allow users to order products, including books and creative materials, and common consumer products such as beer.[677] Examples of such digital helpers are given in the depictions of the smart home hub 'Max' and Internet-connected doll 'Ella' in **Vignettes J3**, **J9**, **J10**, **J11**, **J13**, and **J14**.

A question remains: why does this matter? Consumers have always been on the receiving end of persuasive tactics from advertisers. One argument is that there is a potential significant difference in scale and effectiveness. Although *actual* effectiveness of digital consumer manipulation techniques is not yet proven,[678] and is at times contested,[679] evidence is emerging to support Kim's predictions that:

> in the future the extent and type of information will mean that [advertisers'] inferences may be more accurate, more revealing, and their ability to manipulate consumer behaviour more successful.[680]

Recent empirical research indicates that psychological characteristics:

---

[677] *Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant in Arkansas v Bates (Circuit Court of Benton County, Arkansas, Case No Cr-2016-370-2, 17 February 2017)*; Matt Tate, 'Amazon's New Alexa Update Means It Can Bring You Beer in Two Hours' (*ShortList*, 21 March 2017) <www.shortlist.com/tech/gadgets/you-can-now-tell-amazons-alexa-to-bring-you-a-beer-amazon-echo/18775> accessed 18 December 2018.

[678] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 15; Tal Z Zarsky, 'Privacy and Manipulation in the Digital Age' (2019) 20 Theoretical Inquiries in Law 157, 171.

[679] Antonio Facia Martinez, 'The Noisy Fallacies of Psychographic Targeting' (*Wired*, 19 March 2018) <www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting/> accessed 30 June 2018.

[680] Kim, 'Two Alternate Visions of Contract Law in 2025' (n 89) 312. See also Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 9–12.

1) can be more accurately assessed by online behaviour (than by human-based assessment);[681] and
2) can be used effectively in personalised advertising with the result that targeted consumers will engage significantly more with advertisers and buy more, compared with non-personalised advertising.[682]

The impact of scale will potentially be amplified if and when XDT is implemented at scale in eObjects and the systems in which they participate.[683] The question is: 'at which point [do] digital marketing practices, and in particular if they are based on intrinsic data analysis, opaque algorithms and sophisticated forms of persuasion, turn the normally 'average' consumer into a vulnerable one'?[684]

However, the contention that consumers faced with digital technologies are actually more vulnerable is contested. For example, Peppet argues that a greater availability of information available to consumers enabled by digital technologies can work to a customer's advantage.[685] For example, consumers can now access information about products while in-store, including through review sites that raise specific issues with the quality of products and/or services, as well as onerous contract terms. This allows consumers to more easily work out what firms offer the best deal, over and above price considerations.[686] In contrast, Noto La Diega and Walden challenge Peppet's arguments on the basis of complexity. They argue that both the nature of the technology and the contractual arrangements applying to many eObjects

[681] Youyou Wu, M Kosinski and D Stillwell, 'Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans' (Proceedings of the National Academy of Sciences of the USA, 27 January 2015).

[682] SC Matz and others, 'Psychological Targeting as an Effective Approach to Digital Mass Persuasion' (Proceedings of the National Academy of Sciences of the USA, 28 November 2017).

[683] Hartzog and Selinger, 'The Internet of Heirlooms and Disposable Things' (n 636) 591–92.

[684] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 160.

[685] Peppet, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (n 62) 716–17.

[686] Ibid.

and their supporting services are so complicated that consumers will have serious problems understanding their impact on their purchases and ongoing use.[687] See **section 3.5** of this chapter for a more detailed discussion of complexity.

Also, it is arguable that the greater amount of information that is now available, and the inferences that can be drawn from it, can be used to target people when they actually are in a vulnerable state. In 2017, *The Australian* reported that staff of that newspaper had received a copy of a leaked confidential internal report by Facebook executives. The journalist alleged that the social media company was giving advertisers the opportunity to exploit data on Australian teenagers as young as 14 'to target them at their most vulnerable, including when they feel "worthless" and 'insecure"'. The report also indicated that Facebook had analysed times in a normal week when particular emotions were prevalent amongst teenagers.[688] Facebook subsequently denied that the company had any tools that *targeted* people based on their emotional state.[689] However, the social media company had previously been actively involved in research intentionally attempting to manipulate the emotional states of Facebook users.[690]

It is clear that digital consumer manipulation has the potential to undermine the Consumer Goals of **Choice** and **Fairness**. However, there is also the possibility that the Consumer Goal of avoiding **Disadvantage** may also be

[687] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 4.

[688] Darren Davidson, 'Facebook Exploits "Insecure" To Sell Ads' *The Australian* (Sydney, 1 May 2017) <www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6> accessed 21 May 2018.

[689] Facebook Newsroom, 'Comments on Research and Ad Targeting' (*Facebook*, <https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/> accessed 28 August 2018.

[690] Adam DI Kramer, Jamie E Guillory and Jeffrey T Hancock, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks' (2014) 111 Proceedings of the National Academy of Sciences 8788; Kashmir Hill, 'Facebook Manipulated 689,003 Users' Emotions for Science' (*Forbes,* 28 June 2014) <www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#2f6a79e6197c> accessed 28 August 2018.

compromised. For example, should those with particular 'vulnerability profiles' be able to claim greater protection than the 'average' consumer? For example, societal attitudes are likely to be disapproving towards a marketer who targets a habitual gambler just about to pass a betting shop with an offer of an extended limit on her credit card.[691] Even more likely are serious societal qualms about:

- the impact on public health if marketers are known to target Fahim, a diabetic, with doughnut discounts (**Vignettes F1** and **F4**); or
- the protection of consumers who are minors, such as in the case of the targeting of Mylin, Jessica's nine-year-old daughter (**Vignette J11**).

The attitude might be different, however, towards someone who is persuaded to buy a face cream just because his favourite celebrity's voice is used to persuade him. The question remains whether any of these scenarios are ones which would be considered a type of persuasion from which consumers should be protected.

3.3.2 Data-based discrimination

Attributes and Interactions: **Data collection, data handling, data communication** *Consumer Goal/s:* **Disadvantage, Fairness, Information**

In addition to the targeting of advertising as discussed in **section 3.3.1** of this chapter, data can be used to discriminate against or between consumers. Data can be used to decide whether to offer particular products or services to consumers, or to vary the conditions on which those products or services are offered, dependent on the attributes of the individual consumer.

For example, in the US, health insurers already provide discounts to those who give access to their fitness tracker data, in effect charging a premium to

[691] Although note that this may be regulated under legislation aimed to reduce incidences of problem gambling.

those who do not.[692] Further, discriminatory practices may extend well beyond pricing. Insurers may well refuse cover – or only offer limited cover – to those who refuse access to install a telematics device in their car, which generates personalised data about their driving behaviour (as they do already with discount car insurance).[693] Economically disadvantaged consumers may not be able to afford the relevant product or service without the discount, and therefore will find it impossible to opt out of providing their data. Insurers already have access to a lot of data, but the nature of this data is significantly different,[694] in particular because it is intensive and timely.

Data-based discrimination is not new, is not confined to eObjects, and is a vast topic, in need of multiple dissertations on its own. Some forms of data-based discrimination are already unlawful in many jurisdictions, such as refusing to supply goods or services, or supplying them on less favourable terms, to people of a particular race.[695] However, other forms of discriminatory conduct, such as price discrimination based on data provision conditions, can be engaged in without legal restrictions. The possibility that fundamental human rights can be undermined by both lawful and unlawful discriminatory conduct is real and urgent. However, there is no scope within this dissertation to deal with this issue as a wrong in itself. This section deals with data-based discrimination in the very limited context of discussing the risk of exposure to discrimination of which consumers are not aware.

Data-based discrimination can be deliberate or unintended. One area of particular concern is that of 'algorithmic discrimination', where the often

---

[692] Alan Martin, 'Step and Save: The Truth about Wearables and Health Insurance' (*Wareable*, 21 May 2015) <www.wareable.com/wearable-tech/step-and-save-the-risks-of-using-fitness-tracker-to-save-on-your-insurance-premium-1163> accessed 3 November 2016.

[693] Brian O'Connell, 'Telematics Could Cut Your Car Insurance, But There Are Privacy Risks' (*The Street*, 21 February 2018) <www.thestreet.com/story/14493364/1/telematics-could-cut-your-car-insurance-but-there-are-privacy-risks.html> accessed 11 July 2018.

[694] Rose, Eldridge and Chapin, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (n 63) 35–36.

[695] For example, Racial Discrimination Act 1975 (Cth).

relatively small and/or selective datasets used in machine learning contain societal biases.[696] For example, there is a significant literature emerging relating to algorithmic discrimination on the basis of data collected on race, gender, health status,[697] socio-economic status and other variables,[698] affecting areas such as employment opportunities,[699] housing,[700] policing[701] and sentencing policies,[702] just to name a few. In early 2017, Amazon abandoned its use and further development of a recruiting tool that used machine learning because they had discovered it 'was not rating candidates for software developer jobs and other technical posts in a gender-neutral way'. Allegedly, this was due to the nature of the training dataset used.[703]

[696] Solon Barocas and Andrew D Selbst, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671.

[697] Sharona Hoffman, 'Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease' in Glenn Cohen, Allison Hoffman and William Sage (eds), *Big Data, Health Law, and Bioethics* (CUP 2018).

[698] Sara Hajian, Francesco Bonchi and Carlos Castillo, 'Algorithmic Bias: From Discrimination Discovery to Fairness-Aware Data Mining' (Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, 13 August 2016).

[699] Mark Burdon and Paul Harpur, 'Re-Conceptualising Privacy and Discrimination in an Age of Talent Analytics' (2014) 37 University of New South Wales Law Journal 679.

[700] Ariana Tobin, 'HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse' (*ProPublica*, 28 March 2019) <www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms> accessed 5 April 2019.

[701] Rik Peeters and Marc Schuilenburg, 'Machine Justice: Governing Security through the Bureaucracy of Algorithms' (2018) 23 Information Polity 267.

[702] J Angwin and others, 'Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased Against Blacks' (*ProPublica*, 23 May 2016) <www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 1 May 2018; J Larson and others, 'How We Analyzed the COMPAS Recidivism Algorithm' (*ProPublica*, 23 May 2016) <www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> accessed 8 July 2018. Note, however, that this analysis has been challenged in Anthony Flores, Kristin Bechtel and Christopher Lowenkamp, 'False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased Against Blacks"' (2016) 80 Federal Probation 38.

[703] Jeffrey Dastin, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' (*Reuters*, 10 October 2018) <www.reuters.com/article/us-amazon-

While different forms of discrimination have a long history, the challenge for consumers lies in the fact that inferences drawn from data are often inscrutable or difficult to perceive. Providers may conceal or obfuscate the reasoning behind their decisions without any real prospect of the consumer finding out the 'real' reasons. Additionally, in some cases the inscrutability of the inferences extends even to Providers themselves. Providers may use third party products or services where the third-party refuses to reveal their data collection techniques or processing to protect their commercial investment. It also may be due simply to the design of the process, as machine learning algorithms generally not only do not, but arguably cannot, provide explanations that humans can understand.[704] Transparency of the data relied upon for a decision is 'highly variable, and in some circumstances non-existent'.[705] So a Provider may refuse, or be unable, to reveal the real reasons behind inferences based on data collected by eObjects. This type of challenge is not 'new', but as with digital consumer manipulation, the amount, variety and intimacy of the data collected and distributed via eObjects can contribute both to the ability of Providers to discriminate and the likelihood of accidental or deliberate concealment.

If consumers are not adequately informed about how the data collected by eObjects is used, and particularly if and how it is used to discriminate against them, then this would conflict with the Consumer Goal of providing sufficient **Information** to consumers. Although it is out of scope for this dissertation, it is also worth noting that a 2018 survey of 1004 nationally representative Australian consumers carried out on behalf of the Consumer Policy Research Centre (**CPRC**, **CPRC Survey**) indicated that 67% of respondents believed that government 'should develop protections to ensure

com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G> accessed 23 October 2018.

[704] Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking for' (2017) 16 Duke Law & Technology Review 18, 25.

[705] Roger Clarke, 'Quality Assurance for Security Applications of Big Data' (Proceedings of the European Intelligence and Security Informatics Conference, Uppsala, 17–19 August 2016) 4.

consumers are not unfairly excluded from essential products or services based on their data'.[706] Therefore, it is likely that data-based discrimination can conflict with Consumer Goals of limiting **Disadvantage** and promoting **Fairness.**

3.3.3 Consumer 'lock out'

Attributes and Interactions: **Prevalence, Dependency, Core**

Consumer Goal/s: **Disadvantage**

The **prevalence** of eObjects may lead to a scarcity problem: the manufacture of non-eObject versions of consumer products may become unprofitable, and consumers will become locked out of accessing non-eObject products and services. Consumers may find it impossible to acquire products or services that offer some desired functionality without being also forced to accept some unwanted functionality, such as collection of personal information or other data. Opting out may mean that they lose access to a basic service altogether, as is likely to happen with Kylie's watch (**Vignette K3**). If the product or service is essential, consumers with legitimate concerns about the attributes and interactions of eObjects and their disbenefits, such as in the areas of privacy and security, may nevertheless find it impossible to opt out.[707]

Where **dependency** on remote resources is essential to the functionality of the eObject, this can also lock certain consumers out. Remote, rural and even regional areas in countries like Australia may not have the connectivity required for particular services that require communications between eObjects and remote system elements.[708] If it is not profitable to make non-

[706] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) 37.

[707] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 38–39.

[708] The rollout of the National Broadband Network across Australia may have a positive effect on connectivity. However, 5.5% of Australian households (predominantly in rural areas) will have either a Fixed Wireless or Satellite/Sky Muster connection to the Network. These two types of connections are capable of far lower speeds than those available to other households. Tara Donnelly, 'Complete

eObject versions, then rural and regional residents may have to function without the object at all. Alternatively, like Kylie (**Vignette K1**), consumers who need or desire a particular capability may have to move homes in order to access it. This is particularly problematic in the case of basic services such as healthcare.

It is not unknown for consumer products to be discontinued while some consumers still have a use for them, or for products and services to be difficult to acquire or access in rural and remote areas; so this is not a 'new' problem for consumers. However, the problem is exacerbated by eObjects, particularly in the context of the potential for eObjects to be used to deliver more essential services, such as in healthcare and infrastructure, and consumer objections to excessive data collection, such as Kylie's in **Vignette K3**.

The consumer 'lock out' problem would appear to directly affect the Consumer Goal of limiting **Disadvantage**, in that the lack of availability of eObjects may fail to meet the needs of those who are vulnerable or disadvantaged. It is useful to note here that the United Nations' most recent revision of its Guidelines for Consumer Protection encourage Member States (of which Australia is one) to implement specific policies to distribute 'essential goods and services' in areas where they may not be available, such as rural areas.[709]

guide to the NBN: Your questions answered' (*WhistleOut*, 10 December 2018) <https://www.whistleout.com.au/Broadband/Guides/NBN-Guide-What-You-Need-to-Know> accessed 10 May 2019. Additionally, a large percentage of addresses in Australia's largest cities –Brisbane (62%), Melbourne (42%) and Sydney (55%) –are connected to the Network via hybrid-fibre coaxial, an older technology component which has been the subject of reports substantially questioning its reliability: see Tooran Alizadeh, Edward Helderop and Tony Gubresic, 'Around 50% of homes in Sydney, Melbourne and Brisbane have the oldest NBN technology' (*The Conversation*, 7 May 2019) <https://theconversation.com/around-50-of-homes-in-sydney-melbourne-and-brisbane-have-the-oldest-nbn-technology-115131> accessed 10 May 2019.

[709] United Nations Guidelines for Consumer Protection, GA Res 70/186, UN Doc A/RES/70/186 (adopted 22 December 2015) pt V.E.36(a).

3.4 Post-supply value

Many eObjects return value for Providers that is additional and separate to the up-front price paid for the underlying object, in contrast to many non-eObject consumer products. For example, a refrigerator which is not an eObject delivers little post-sale value for its supplier, primarily a reputational effect from consumer ratings. However, Providers maintain significant post-sale *obligations* in the form of warranties, which can give rise to significant liabilities for Providers. The minimal value traditionally returned to Providers post sale has meant that consumers have historically faced challenges in relation to obtaining timely and good quality post-supply services, even where express warranties are available.[710]

However, the potential for post-sale value in eObjects is much more significant.[711] This value often lies in post-supply contracts for services with ongoing fees, or in the data which is collected and communicated.

For example, Jessica's smart refrigerator (**Vignette J2**) may deliver post-sale value to Providers in the following ways:

- data on use and consumption patterns, which may be on-sold to supermarkets to inform advertising campaigns (including personalised advertising) or to white goods manufacturers for use in design;
- ongoing licence and service fees, such for software maintenance and updates, and/or cloud data processing and handling;
- commissions from partner supermarkets when orders are made; and
- effective brand loyalty, once consumers looking to buy a new refrigerator realise that if they switch brands they may need to re-enter all of their ordering data, or that an alternative refrigerator is not compatible with

[710] Stephen Corones, 'Consumer Guarantees in Australia: Putting an End to the Blame Game' (2009) 9 Queensland University of Technology Law and Justice Journal 137, 139–42.

[711] Kate Carruthers, 'How the Internet of Things Changes Everything: The Next Stage of the Digital Revolution' (2014) 2 Australian Journal of Telecommunications and the Digital Economy 69.1, 69.5.

some of their other connected home systems and/or applications (a form of consumer 'lock-in'[712]).

The availability of this increased post-supply value *may* prove to be an incentive to Providers to improve product longevity and post-supply services to consumers. However, it can also lead to challenges for consumers (and others, such as renters of smart homes) in relation to data awareness, data portability and the nature and extent of post-supply restrictions.

3.4.1 The value of data

Attributes and Interactions: **Core, Prevalence, Visibility, Mobility, Portability**

Consumer Goal/s: **Information, Redress, Choice, Fairness**

Data protection and privacy issues dominate the scholarly and popular literature on eObjects. To deal with all of these issues is outside the scope of this dissertation, particularly as other Australian scholars and industry commentators have already provided some significant discussion.[713] This section's focus is on data gathering practices by Providers that have a direct impact on consumer contracts.

Consideration for eObjects in a consumer transaction is often not confined to a monetary price.[714] The most common alternative form of consideration is

[712] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 47. For more information on consumer 'lock-in' in contexts outside of eObjects, see W Brian Arthur, 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events' (1989) 99 The Economic Journal 116; Joseph Farrell and Paul Klemperer, 'Coordination and Lock-in: Competition with Switching costs and Network Effects' in Armstrong M and Porter R (eds), *Handbook of Industrial Organization*, vol 3 (Elsevier BV 2007).

[713] For example, Li, 'Deciphering Pervasive Computing: a Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' (n 55); Richardson and others, 'Privacy and the Internet of Things' (n 56); Richardson and others, 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' (n 56); Caron and others, 'The Internet of Things (IoT) and Its Impact on Individual Privacy: An Australian Perspective' (n 102); Bosua and others, 'Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective' (n 102); Vulkanovski, '*Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers* (n 63); Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56) 158–93.

[714] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 193–94.

consent to the acquisition and use of personal data. The demand for data did not begin with eObjects. However, the greater amount of data collected by eObjects, based on the **prevalence**, **mobility** and/or **portability** of such objects, considerably increases the likelihood of Providers requiring access to data as a non-negotiable part of the consideration for supply and services contracts. Where eObjects embody partially or fully invisible data gathering processes, consumers may not be aware of the extent to which data is being collected, or that any is being collected at all. Even in older technologies, the lack of awareness of consumers is significant. The CPRC Survey results indicated that only 47% of respondents realised that many smartphone applications are capable of collecting data that is unrelated to the function of the application.[715] This is despite the fact that there is considerable evidence that many mobile applications actually do this.[716]

Therefore, there are two significant challenges for consumers in relation to the data demanded by Providers as part of the supply of eObjects. In order to meet the Consumer Goals of **Information** and **Choice**, consumers should be:

1) aware of what data is being collected, to whom it will be provided, and for what purpose ('**data awareness**'), as differences between the data requirements of competing products is relevant to consumer choice; and
2) able to take their data with them if they terminate their use of the original eObject, for example to buy another eObject of a competing brand ('**data portability**').

3.4.1.1 Data awareness

The challenges that consumers face in relation to data awareness are:

[715] Nguyen and Solomon, *Consumer data and the digital economy: emerging issues in data collection, use and sharing* (n 646) 29.

[716] Wolfie Christl and Sarah Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (facultas 2016) 49, reporting that 31% of 1200 popular mobile applications accessed data that was not required for the application to operate.

- the data capable of being collected may not be obvious to the consumer; and
- suppliers may give inadequate details as to the data collected and its subsequent use.[717]

Currently, on a standard e-commerce website, consumers consciously enter data in the form of text. This may include, for example, name, address and credit card details. Tracking cookies[718] can also pull some additional data from the consumer without active entry. However, when Fahim goes for a jog with his smart watch and his insulin pump (**Vignette F1**), or when Jessica blows into the breathalyser on Kitt (**Vignettes J1, J7**), they are most likely viewing themselves as performing physical activities such as jogging, or injecting insulin, or breathing out. They are not consciously providing information to a third party as they do when they fill in a website form. It is currently unlikely that Jessica will contemplate that the breathalyser data will be subpoenaed as highlighted in **Vignette J8**. However, this may change over time as court cases are publicised where such applications are successful. For example, it was reported in May 2018 that a US electricity company had received subpoenas from government agencies relating to smart meter data at 480 residences and business premises in the previous year.[719]

Low **visibility**, particularly of the data collection function, creates a danger that consumers will consider that the eObject they are using 'is merely a good like any other – akin to a stapler or ballpoint pen – rather than a data source and cloud-based data repository.'[720] It is likely, therefore, that the type

[717] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 193–94.

[718] Kate Mathews-Hunt, 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (2016) 32 Computer Law & Security Review 55.

[719] Daniel Zwerdling, 'Your Home is Your … Snitch?' (*The Marshall Project*, 24 May 2018) <www.themarshallproject.org/2018/05/24/your-home-is-your-snitch> accessed 11 September 2018. In 2017, Amazon contested a subpoena for data collected by an Amazon Echo smart speaker relating to a murder charge, but the defence ultimately agreed to the disclosure of the recordings and the case was dropped: Kathleen Zellner, 'The Internet of Things and the Law' (ABC Radio National, *The Law Report*, 6 March 2018).

[720] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 90.

of data that has the potential to be collected by Providers is significantly less obvious than that previously collected online, and significantly exacerbates the challenge of data awareness for consumers. This is despite the fact that a user's need to know what data is being collected and how it is being used in relation to such eObjects is arguably greater than in traditional e-commerce. This greater need is due to eObjects' greater potential to gather data about a purchaser and the people with whom they interact.

An example of this problem has already attracted litigation in the US. In 2016, Illinois consumers brought a class action against Standard Innovation (US) Corp, the manufacturer of the 'We-Vibe' vibrator. Consumers and their partners could pair the We-Vibe via Bluetooth with a smartphone to allow for remote control of the device. The plaintiff in the Illinois action alleged that the manufacturer programmed the smartphone app to:

> secretly collect intimate details about its customers' use of the 'We-Vibe', including the date and time of each use, the vibration intensity level[,] … mode or pattern selected by the user … and … the email address of We-Vibe customers … allowing [Standard Innovation] to link the usage information to specific customer accounts.[721]

The complaint alleged this was done without consumers' consent or knowledge, and made the obvious point that most customers would not have bought the We-Vibe if they had known about this data collection.[722] The litigation was settled on 9 March 2017, for CAD5 million.[723]

Suppliers commonly use privacy policies to deliver information about data collection and use, often separately from other terms and conditions. Yet this information may not be readily available at the time of purchase, and it is often difficult to discover (see discussion of 'Contract Distancing' in **section 3.5.1.2** of this chapter). The form factor of some eObjects, such as

[721] Complaint, *NP v Standard Innovation (US) Corp,* Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois (Filed 2 September 2016) [19].

[722] Ibid [23].

[723] Class Action Settlement Agreement, *NP v Standard Innovation (US) Corp,* Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois (Filed 9 March 2017).

small or no screens, make it difficult as a practical matter to display privacy policies and other terms on many eObjects themselves. However, early indications are that suppliers are not packaging hard copy privacy policies with the physical eObject, or including an electronic display of terms when associated apps are required to be downloaded.[724] Many suppliers will have some form of privacy policy on their website, but there are two problems:

- if eObject purchasing and use activities are completely disconnected from the data-gatherer's website, then it seems insufficient that the only notification is contained there; and
- early indications are that even where a privacy policy exists on the supplier website, often the drafting is directed towards the website itself and not tailored to the eObject.[725]

The common practice of updating privacy policies simply by changing the website without notifying consumers can also lead to problems of a lack of data awareness.

Also, there is a question around enforceability. The Privacy Act requires that many (but by no means all) businesses have a privacy policy[726] containing specified information,[727] and this requirement is also quite common in other jurisdictions outside Australia. However, these legislative regimes are routinely criticised for ineffectiveness in ensuring first, that privacy policies contain useful information, and second, that breaches are enforceable.[728] Privacy policies do not necessarily form part of the contractual terms and

[724] A recent survey of 20 popular consumer eObjects ranging from fitness trackers to breathalysers to home automation systems found that none contained a privacy policy packaged with the object, or any indication where one could be located. Even in the downloading step, many did not provide a privacy policy or any indication of where to find one: Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 144–46.

[725] Ibid 146.

[726] Privacy Act 1988 (Cth) sch 1, Australian Privacy Principle 1.3.

[727] Ibid sch 1, Australian Privacy Principle 1.4.

[728] A long list of articles critical of privacy policies can be found in Roger Clarke, 'The Effectiveness of Privacy Policy Statements' in D Kerr, J Gammack and K Bryant (eds), *Digital Business Security Development: Management Technologies* (IGI Global 2011).

conditions, so a remedy for contractual breach is not automatically available. Recent empirical research carried out in Australia has confirmed that there are many practical barriers to the effectiveness of privacy policies to protect consumers. Most consumers do not read them. Even when they do, they overwhelmingly accept terms that they are uncomfortable with because they feel they have no bargaining power if they wish to make a purchase:[729] that is, the terms are 'take it or leave it'.

Inadequate or misleading statements on what and how data is to be used will conflict with the Consumer Goal of **Information**. The inability to negotiate data collection and subsequent use conditions conflicts with the Consumer Goals of **Choice** and **Fairness**. The lack of enforceability around the claims made in these statements compromises the Consumer Goal of **Redress**.

3.4.1.2 Data portability

One risk of data-rich eObjects is that their lack of 'data portability'[730] may result in users being effectively 'locked in' to one device or one brand. This risk arises when useful data collected by one eObject is not practicably portable to a substitute eObject. This may be due to:

- Providers not storing it, or refusing to release it to the consumer;
- the design of the eObject and/or accompanying system (either deliberately or inadvertently) not allowing for easy extraction of data in a format that is compatible with other eObjects or systems.

Data portability may also only be offered subject to conditions: for example, that the original Provider is allowed to keep a copy of the customer's data even when the customer has moved on.

[729] Consumer Policy Research Centre, 'Data Protection Rules Are Failing Australian Consumers' (Fact Sheet, 2018) <https://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy/fact_sheet_-_data_protection_rules_failing_australian_consumers/> accessed 23 May 2018.

[730] Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87) 31; Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 37–38.

This challenge is not confined to eObjects, but is exacerbated by the sociotechnical change brought about by eObjects. Data portability has already been raised as a significant issue in relation to a number of areas, such as social media platforms,[731] and the retail banking, energy and telecommunications sectors.[732] What makes this challenge more significant in relation to eObjects is the scale and relative importance of data to a consumer's daily life. At present a consumer may regularly use one or two social media platforms, but as eObjects become more prevalent, they may use tens or hundreds of them in their daily life. eObjects are also used for a variety of different purposes, some of which are easily dispensed with, but others of which are not (such as medical devices or disability aids). Costs of portability may also be much higher, such as those involved in moving from one integrated home system to another.

If data is not practicably portable, a consumer's decision to buy an alternative eObject to replace the original one may be affected. If the data is important to the consumer, she may decide it is impossible or too much trouble to buy a competing brand, and instead buy the upgraded version of her old eObject.[733] For example, if Fahim needs to replace his insulin pump (**Vignette F1**), or Kylie her health monitor (**Vignette K1**), difficulty in importing data to a new system will most likely play a very large part in their choice of a replacement.

If the consumer was not given sufficient notice of the lack of data portability at the time of the original purchase, then this causes a problem for the Consumer Goal of **Information**. Even if the consumer received sufficient information at the time the contract was entered into, competition may still be affected. This would be the case if the original product was the first on the

[731] Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193.

[732] Productivity Commission, *Data Availability and Use* (n 77).

[733] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 38.

market, and the manufacturer attempted to protect its investment by use of a 'walled garden',[734] for example by placing restrictions on interoperability (as discussed in **section 3.5.2** of this chapter). This would constitute an attempt to restrict freedom of choice by consumers, and therefore would be in breach of the Consumer Goal of **Choice**.

The Australian Government has recently recognised, at least in part, the importance of data portability to consumer choice (although not specifically in the context of eObjects). On 31 March 2017, the Productivity Commission recommended the introduction of a 'Consumer Data Right' (**CDR**).[735] In May 2018, the Federal Government announced that it would be introducing this CDR into the CCA.[736] On 15 August 2018, the government released an exposure draft of the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) and Exposure Draft Explanatory Materials. The CDR is intended to provide a right for consumers to require data portability from commercial entities in order to 'improve consumer control over the data which businesses hold about [them,] … make it easier for them to find a better deal and share their information only with partners they trust'.[737] However, the CDR in its currently proposed form provides a very limited right. Treasury, the Office of the Australian Information Commissioner (**OAIC**) and the ACCC have begun public consultation[738] with regard to the introduction of the CDR to the banking, energy and telecommunication sectors first. This is proposed to be followed by other sectors 'over time'.[739] Therefore, the

[734] Ibid.

[735] Productivity Commission, *Data Availability and Use* (n 77) 199.

[736] Australia, Department of Prime Minister and Cabinet, *The Australian Government's Response to the Productivity Commission Data Availability and Use Inquiry* (1 May 2018) <http://dataavailability.pmc.gov.au/sites/default/files/govt-response-pc-dau-inquiry.pdf> accessed 28 May 2018, 6.

[737] Ibid.

[738] For example, the author of this dissertation attended a meeting held by Treasury, the OAIC and the ACCC with representatives from the Consumer Data Research Network on 18 May 2018 at ACCC offices in Sydney, Melbourne and Brisbane, to discuss implementation of the Consumer Data Right.

[739] Australia, Department of Prime Minister and Cabinet, *The Australian Government's Response to the Productivity Commission Data Availability and Use Inquiry* (n 736) 6.

inclusion of eObjects outside the initially named sectors may be possible in the future.

3.4.2 Post-supply restrictions

Attributes and Interactions: **Core, dependency, volatility**
Consumer Goal/s: **Fairness, Information**

Some form of software is integrated into every eObject. Some types of eObjects, such as eBook readers and networked media players, will also contain a substantial amount of digital content aside from software. **Volatility** of resources in many eObjects (particularly limitations in processing power and data storage) also mean that data processing and storage may well be accomplished outside of the original eObject, leading to significant **dependencies** on remote services and/or infrastructure.

Post-supply restrictions on the consumer may arise in many different ways. These include:

- consumers may be required to enter into an ongoing service contract with the original supplier or another Provider, such as for cloud data processing and storage;
- the eObject may not be 'sold' to the consumer, in terms of granting full transfer of property rights. Rather, the supply contract may be one of lease or licence, which is likely to include an obligation to return the eObject on breach or termination of the lease/licence contract.[740] Alternatively, there may be a mix of property rights granted;
- the supply may be subject to restrictive licence terms for the software or other digital content. These terms may restrict copying, modification or particular types of use. Sometimes these are included in the supply agreement itself, or else in separate agreements such as End User Licence Agreements, Acceptable Use Policies and/or Terms of Use (**TOU**). These terms may also effectively prevent resale of the eObject, even if property

[740] Walker Smith, 'Proximity-Driven Liability' (n 59) 1815–16; Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (n 61) 83; Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87) 16.

in the physical device is transferred outright. For example, the EULA for Blink's connected security camera stated that:

> You agree not to, and you will not permit others to, (a) license, sell, rent, lease, assign, distribute, transmit, host, outsource, disclose or otherwise commercially exploit the Product Software or make the Product Software available to any third party.[741]

- the technical set-up of the eObject may impose mandatory and irreversible personalisation of the eObject (such as usernames, or an inability to delete data) that may limit its resale attractiveness.[742]

Challenges for consumers arising out of these post-supply obligations include:

- post-supply notification of undesirable and even unacceptable terms where consumers are not made aware at the time they ordered the eObject that the post-supply obligations would apply or be mandatory, such as when an agreement to a EULA is required as part of the post-purchase set-up process;
- greater restrictions on use, particularly compared with a non-eObject version of the same physical object;
- greater restrictions on resale by consumers even when the physical eObject is owned and not leased or licensed, as the EULA on software essential to the functionality of the eObject may be non-transferable;[743] and
- more significant penalties for breach of use restrictions, including criminal remedies such as those contained in anti-hacking[744] and/or copyright legislation, as opposed to civil remedies for contractual breach.

For example, if Jessica wishes to undertake her own repairs to Kitt (**Vignette J6**), she will most likely need to access integrated software, and face both legal and technical barriers to doing so. A similar problem exists in

[741] Blink, 'End User License Agreement' <https://blinkforhome.com/pages/eula?locale=en> accessed 26 April 2019.

[742] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 201.

[743] Although it is likely black markets will continue to exist unless and until software suppliers win the war on digital rights management technologies.

[744] Walker Smith, 'Proximity-Driven Liability' (n 59) 1815–16, fn 313.

relation to the repairs needed to Fahim's automated vacuum cleaner (**Vignette F6**). Software modification without Provider consent will in many cases constitute a breach of the EULA and/or copyright legislation. Modification may also be technically impossible without circumventing technological protection mechanisms (**TPMs**), often an illegal act in itself in jurisdictions signatory to and compliant with the WIPO Copyright Treaty.[745] Providers might also use their remote disablement capacity (see **section 3.2** of this chapter) in private enforcement conduct, such as disabling software for a perceived breach of copyright law or contractual conditions.[746]

These challenges arising are not merely theoretical. For several years, US farmers have been disputing the attempts of Deere & Company (**John Deere**) and other manufacturers to restrict their rights to repair their agricultural machinery, which contains embedded software and TPMs.[747] In 2015, against the objections of John Deere and others,[748] the US Copyright Office granted a three-year exemption[749] for vehicle software modification to the anti-circumvention provisions of the Digital Millennium Copyright Act (**DMCA**).[750] A year later, John Deere issued a licence agreement which prohibited almost all software modification and circumvention of TPMs.[751]

---

[745] World Intellectual Property Organization, Copyright Treaty, opened for signature 20 December 1996, entered into force 6 March 2002. Article 11 of the Treaty requires signatories to provide adequate legal protection and remedies against TPMs.

[746] This possibility was suggested by an anonymous reviewer at the *Oxford University Commonwealth Law Journal*.

[747] Jason Koebler, 'Why American Farmers Are Hacking Their Tractors with Ukrainian Firmware' (*Motherboard*, 22 March 2017) <https://motherboard.vice.com/en_us/article/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware> accessed 1 May 2017.

[748] US Copyright Office, *Section 1201 Exemptions to Prohibition Against Circumvention ofTechnological Measures Protecting Copyrighted Works: Second Round of Comments, Proposed Class 21: Vehicle software – diagnosis, repair, or modification*.

[749] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies: A Rule by the Copyright Office, Library of Congress on 10/28/2015.

[750] Digital Millennium Copyright Act, 17 USC § 1201(a)(1) .

[751] John Deere, 'License Agreement for John Deere Embedded Software' (28 October 2016) <www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf> accessed 27 April 2017 sections 4 and 5.

This agreement appears to be an attempt to replace its DMCA rights with contractual rights[752] and ensure that all repairs were done by John Deere contractors. Other car manufacturers in the US have already indicated that they intend to use copyright to prevent amateur mechanics modifying their cars.[753] Circumvention of TPMs in mobile phones ('jailbreaking') is already commonplace:[754] it is likely that the practice will extend to many other eObjects, so this issue may arise in many other contexts. It is worthwhile to note that Australian copyright legislation also prohibits the circumvention of TPMs, imposing significant penalties with only limited exceptions.[755]

The scope of this 'erosion of norms around ownership and control'[756] is significantly different from what has gone before, although it also raises some traditional issues around the feasibility of regulation and market efficiency in the area of post-supply restrictions. Suppliers and others in the provider network will need to make consumers aware of any post-supply restrictions on use in order to comply with the Consumer Goal of **Information.** Unreasonable restrictions on post-supply use will also compromise the Consumer Goal of **Fairness**.

3.5 Complexity

Challenges for consumers arise from the complexity of:

- the technology itself; and

[752] Koebler, 'Why American Farmers are Hacking Their Tractors with Ukrainian Firmware' (n 747).

[753] Pete Bigelow, 'Car Companies Say Home Repairs Are "Legally Problematic," Seek Copyright Restrictions' (*Autoblog,* 20 April 2015) <www.autoblog.com/2015/04/20/automakers-gearheads-car-repairs/> accessed 10 September 2018.

[754] Renai LeMay, 'Locked Down: Foxtel Blocks Non-Samsung Android, Jailbroken Apple Devices' (*Delimiter,* 17 July 2013) <https://delimiter.com.au/2013/07/17/locked-down-foxtel-blocks-non-samsung-android-jailbroken-apple-devices/> accessed 27 February 2019.

[755] Copyright Act 1968 (Cth) ss 116AN, 116AQ.

[756] Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 34.

- the contractual arrangements surrounding the supply of eObjects and the systems in which they participate.

The core attributes of an eObject mean that there is no such thing as a 'simple' eObject. Some are simpler than others, but even the most basic eObject is a hybrid of software, hardware and physical object, and includes at least one sensor.[757] Many eObjects and the systems in which they participate also include one actuator, and are **dependent** on additional services, which are often supplied by more than one Provider. The **interactions** that eObjects have with living things, the physical world, other eObjects and/or other computing devices and systems also add to this complexity. Systems with nested and/or multiple eObjects, or multiple eObjects interacting with conventional computing (such as smart homes) can be very complex, both technically and in terms of associated service contracts to support their functionality.

As discussed in **section 2.1** of this chapter, the nature of eObject ecosystems increases the likelihood that numerous actors will be involved in the provider network. This will mean that the contractual arrangements, and therefore liability allocation, will also be complex. A complex network means complexity in contractual arrangements and, therefore, greater difficulty in allocating liability when things go wrong. Even a basic eObject such as a thermostat may require many separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale, distribution and rental.[758] These contracts may be with separate entities, some having no connection with (or knowledge of) others in the network.[759] Consumers may not even be aware of many of the contracts, as some will only be between two or more Providers. The identity of Providers may well change throughout the

[757] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 8; Coll and Simpson, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (n 63) 33.

[758] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 4–6.

[759] Millard, Hon and Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (n 87) 7.

effective life of the relevant eObject/s and systems through acquisition, restructuring, outsourcing or insolvency. Enforcement rights against the most desirable litigation targets in a provider network may be unavailable to consumers due to privity of contract and the use of subsidiaries with limited equity as contracting parties.

The complexity of the contractual arrangements within a provider network can make it difficult just to *identify* all applicable contracts, let alone interpret them for both end-consumers (including enterprises) and Providers.[760] For example, the Nest thermostat (discussed in **section 2.1** of this chapter) is sold subject to at least 13 different documents containing information on the 'rights, obligations and responsibilities of the various parties' in the provider network.[761] The possibility of conflicting terms and conditions[762] within those documents is also high, as is uncertainty regarding their effects. For example, the sets of terms and conditions purported to apply to sales of the Amazon Dash Button (see **section 3.5.1.2** of this chapter) contain limitation of liability clauses that conflict with each other. One clause attempts to limit liability to zero,[763] the other to USD50.[764] Something as complex as the smart home systems installed in Everyware Place (**Vignette E1**) would in all probability be subject to many more contracts.

[760] Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 3.

[761] Ibid 6.

[762] Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87) 16; Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 13–14.

[763] Amazon, 'Conditions of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=201909000> accessed 11 July 2018, clause entitled 'Disclaimer of Warranties and Limitation of Liability'.

[764] Amazon, 'Amazon Dash Replenishment Terms of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=201730770> accessed 12 July 2018, clause entitled 'Disclaimer of Warranties and Limitation of Liability'.

3.5.1 Making an informed choice

Attributes and Interactions: **Core, dependency, visibility, autonomy**
Consumer Goals: **Information, Fairness**

Consumers, when entering into contracts, require sufficient, accurate and intelligible information on the nature, features[765] and **dependencies** of the product they are buying, in order to meet the Consumer Goal of **Information**. This requirement can be met with the supply of minimal information when acquiring a *simple* product. However, a consumer buying a complex eObject or eObject ecosystem, particularly one which requires additional services to function, will need more than minimal information in order to make a sensible purchasing decision. The information required might include such things as interoperability limitations, resource constraints, ongoing service fees and licensing conditions. Mere provision of information about the supplied product and/or service is insufficient. In order to make an informed choice, the consumer should know about the alternatives on offer,[766] and be able to make a considered judgment of the price and quality differences between possible alternatives.[767]

Consumers face three challenges to receiving adequate **Information** to foster effective competition:

1) the type of information that is required (content);
2) when and how the information is provided (delivery mechanism); and
3) whether the consumer can adequately understand the information provided, in terms of completeness, complexity and volume (intelligibility).

[765] Browne and others, 'Protecting Consumers from Themselves: Consumer Law and the Vulnerable Consumer' (n 675) 159.

[766] Ibid.

[767] Productivity Commission, *Review of Australia's Consumer Policy Framework* (n 420) vol 2, 28.

3.5.1.1 Content

The most important types of information that should be provided to the consumer are:

a) the functionality and interoperability of the eObject, including any limitations (see **section 3.5.2** of this chapter);
b) the full **consideration** both for the eObject and any associated software and services. This information should include details of both monetary and non-monetary consideration, and details of both up-front and periodic payments, with a reasonable estimate of the full amount to be paid over the whole-of-expected-life of the eObject (see **section 3.5.3** of this chapter);
c) any **conditions** on use outside of price (for example, requirements to provide data, AUP, access to premium services) (see **section 3.4** of this chapter); and
d) what means of **redress** exist if loss does ensue, including against whom, and any procedural barriers or limits to reparation (see **sections 3.5.4** and **3.5.5** of this chapter).

All of these types of information are important to a consumer's informed choice for any type of consumer product, so this is not a new challenge. However, the complexity of eObjects compared to the non-eObject versions of similar products, particularly in the associated provision of services, means that this challenge is likely to be exacerbated in the eObject context, particularly when considering functionality and interoperability (see **section 3.5.2** of this chapter).

3.5.1.2 Delivery mechanism

> Behavioural economics has demonstrated that … the manner in which information is presented and the way that choices are framed can significantly influence marketplace choices, sometimes in ways that are not in the best interests of a consumer.[768]

[768] OECD, *Consumer Policy Toolkit* (OECD Publishing, June 2010) 10.

A clear theme of early visions[769] of ubiquitous computing was the idea that technology should merge into the background. An eObject or associated system may be designed so that interactions are **invisible** or at least unobtrusive. This is often achieved by removing or miniaturising text-supporting interfaces such as screens. Such interfaces cannot practically be used to deliver most contractual terms and conditions.

In some cases, this does not matter overmuch. A hyperlink to contractual terms and conditions can be easily provided when an eObject is ordered online, or printed terms and conditions can be provided over the counter or in the box for a brick-and-mortar purchase. However, in other cases, the contractual processes surrounding the purchase of eObjects bring with them the likelihood of a significant 'lack of proximity between consumers, contract terms and the contract formation process'.[770] This is a phenomenon Elvy labels 'Contract Distancing'.[771] Contract Distancing practices lead to an outcome where consumers may enter into contracts with a significant limitation on their access to terms and conditions. Consequently, the reduced ability to understand the bargain they are entering into presents a substantially new challenge for consumers. It is also common for Providers to include a term in the contract allowing for unilateral amendment by Providers, often without any notice other than a change in the terms displayed on the Provider's website. Therefore, Contract Distancing practices are seen not only in the initial contract formation process, but also in the case where unilateral amendments are made by Providers.

Jessica's Wulwurths AutoBuy (**Vignette J2**) is based on the real-life Amazon Dash Button. The Dash Button is an Internet-connected button that, when pressed, places an order for the product displayed from a partner retailer.

[769] Weiser, 'The Computer for the 21st Century' (n 19) 94.

[770] Elvy, 'Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond' (n 94) 843.

[771] Ibid.

Figure 5: Amazon Dash Button for Tide washing detergent[772]

For reordering buttons such as the Dash Button, as with many eObjects, the initial acquisition involves a set-up step which requires visiting a website, where terms and conditions are displayed as a clickwrap or browsewrap agreement.[773] For example, acquisition of a Dash Button in mid-2018 from the Amazon website was made subject to the following terms:

- Amazon Dash Replenishment Terms of Use;[774]
- Amazon Device Terms of Use;[775]
- Amazon.com Conditions of Use;[776] and
- Amazon.com Privacy Notice.[777]

Like many online terms and conditions, the Amazon Dash Button terms expressly allow for unilateral amendments to those terms, including the

[772] Amazon, 'Tide Dash Button: Save 5% on All Products Ordered through This Button' (n 529).

[773] For a discussion of clickwrap and browsewrap agreements, see Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (n 36).

[774] Amazon, 'Amazon Dash Replenishment Terms of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=201730770> accessed 12 July 2018.

[775] Amazon, 'Amazon Dash Terms of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=202002080> accessed 11 July 2018.

[776] Amazon, 'Conditions of Use'.

[777] Amazon, 'Amazon.com Privacy Notice' <www.amazon.com/gp/help/customer/display.html?nodeId=468496> accessed 11 July 2018.

price of the product being ordered.[778] Amazon's only obligation regarding these variations is to post amended conditions on the website. Since there is no display mechanism on the Dash Button itself, it is unlikely that Amazon will provide any other form of notification to consumers when varying the terms of the contract with the consumer.[779]

In the Amazon example above, terms and conditions for the initial contract were not subject to significant Contract Distancing (in contrast to variations). However, a clear delivery of the full terms before purchase is by no means ubiquitous in eObjects. Consumers may be given the price up-front when they first purchase the product, but may not be presented with other terms and conditions (such as EULAs, service agreements and maintenance agreements) until well through the set-up process: that is, after the product has been ordered, delivered, unpacked and partially or even fully set up.[780]

Therefore, a consumer may well face challenges in finding out the terms and conditions applicable to their eObject and the systems in which it participates, particularly in relation to the use of data. For example, Peppet's 2014 survey of 20 commercially available consumer eObjects (including fitness monitors, connected breathalysers and power meter trackers) found that suppliers had not included anything in the box or packaging relating to data, privacy or security for any of these products.[781] Even in cases where the relevant terms and conditions were displayed on the website, many of these were bought in brick-and-mortar stores. Without a clear indication that the purchase was subject to further terms and conditions, a consumer could buy these eObjects without any knowledge of those particular terms.

[778] For example, Amazon, 'Amazon Dash Replenishment Terms of Use' (n 774) cl 2; Amazon, 'Amazon Dash Terms of Use' (n 775) cl 3c.

[779] Elvy, 'Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond' (n 94) 879.

[780] For example, in mid-2018 the Nest.com site did not present any terms and conditions (other than price) before the payment page was reached.

[781] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (n 88) 141, App 1.

If consumers are not receiving proper notification of contractual terms due to Contract Distancing, then this may be a breach of the Consumer Goal of **Information**. If Contract Distancing is in operation, the notification is a number of steps removed from the actual transaction, such as when an eObject is purchased in a brick-and-mortar store but the terms and conditions are delivered on the manufacturer's website. In this circumstance, a question about the Consumer Goal of **Fairness** may also be raised. **Fairness** is further compromised if Contract Distancing is combined with a right to unilateral amendment by a Provider without a corresponding consumer right to terminate without penalty or without recovery of costs, such as in fixed-term contracts.

3.5.1.3 Intelligibility

An additional informational challenge inherent in complexity is that 'consumers cannot make well informed decisions when they are presented with information that is incomplete, misleading, overly complex or too voluminous'.[782] Opaque wording and technical terms are the norm for software and hardware contracts. Initial research indicates that this has not changed for eObjects.[783] The content of the information provided may be accurate, but if it is not intelligible to the average consumer, then it is insufficient as a basis for an **informed** choice.

Intelligibility of technical information related to eObjects is not the only problem. Consumers also find contractual terms and conditions difficult to understand.[784] Careless drafting practices can add to the problem of intelligibility. For example, terms and conditions applicable to contracts involving eObjects have already been identified where wording has obviously been written for different (often older) technologies and has not been

[782] OECD, *Consumer Policy Toolkit* (n 768) 10.

[783] See the analysis of the Nest thermostat contractual arrangements in Noto La Diega and Walden, 'Contracting for the "Internet of Things": Looking into the Nest' (n 94) 6ff.

[784] Ibid 3, 9.

properly redrafted for eObjects.[785] There is also a common practice in information technology contracts of using wording drafted for one jurisdiction in contracts made subject to the laws of another jurisdiction. For example, US standard drafting is commonly used in European[786] and Australian[787] contracts, even when it is not particularly suited to the task. This is not a new phenomenon and falls into a category of challenge that is 'in common' with other IT products and services. However, like issues around intelligibility of technical information, this challenge may become much more significant as the use of eObjects – especially complex eObjects – spreads.

3.5.2 Functionality and interoperability

Attributes and interactions: **Dependency, volatility, visibility**
Consumer Goals: **Information**

Consumer knowledge of the **functionality** of the device, system or product–service package acquired is important, as well as its suitability for the consumer's particular purposes. Knowledge of 'normal' functionality will usually be insufficient for a consumer's purposes, particularly where dealing with eObjects with significant **volatility** and/or **dependencies**. Such eObjects will face significant limitations on functionality in particular situations, for example their use in areas with weak network connectivity.[788]

Knowing exactly what the eObject does is not only important for consumers in assessing whether it meets their needs. It is also important because the post-supply value of eObjects (particularly in relation to data collection and communication) can provide an incentive to manufacturers to include features that are beneficial to one or more Providers, but are a disbenefit to the consumer. This can affect their decision about buying the eObject. For

[785] Ibid 3.

[786] Ibid.

[787] This observation is from the author's own experience as a solicitor in Australia specialising in commercial negotiation of information technology contracts.

[788] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93) 191–92.

example, a common (although non-core) attribute of eObjects is **geo-locatability**. However, in many cases that feature is not necessary for the normal operation of the eObject, or at least its communication to a Provider data store may not be necessary. Such functionality may well be **invisible** or unobtrusive. Therefore, an overt disclosure of this 'dark'[789] functionality may need to be formally required, otherwise consumers may remain unaware.

The attribute of **dependency**, and the nature of the interactions that eObjects have, means that specific information on interoperability will also usually be critical. Fahim certainly would not have bought the particular kettle he purchased (**Vignette F5**) if he had been aware of the interoperability problem. Knowledge that the security upgrade to Fahim's phone discussed in **Vignette F3** would cause interoperability problems with his insulin pump may have affected Fahim's decision to install the upgrade or purchase another phone. Further problems can arise where information is incomplete or missing. For instance, imagine that Fahim's problem was not that the kettle was completely incompatible, but that he was not told at the time of purchase that it was only usable when connected to his mobile network, incurring a much higher cost than his smart home network. This would cause a conflict with the goal of **Information**.

3.5.3 Consideration

Attributes and interactions: **Dependency, Use pattern**
Consumer Goals: **Information**

Ensuring that consumers have knowledge of the *full* consideration required to purchase an eObject is an additional challenge. Consideration is more than the up-front monetary price paid for the initial supply. It also includes any follow-on costs, such as purchase of additional applications, periodic subscription fees for service agreements (with associated price increases), or the cost of consumables. This challenge is not completely new, as it appears

[789] This term is adopted from the 'dark scenarios' terminology used in the SWAMI research project, reported in Wright and others (eds), *Safeguards in a World of Ambient Intelligence* (n 238).

in conventional IT contracts, and in some consumer products with associated consumables, such as printers or coffee machines. In the last few years, obfuscation of the true price through drip-feeding of additional costs in the online selling price has also attracted the attention of the consumer regulator, the ACCC. Multiple regulator interventions have occurred as a result of additional fees and charges charged by travel providers.[790] This issue is distinct from whether or not the total price is **fair**, which is a problem for any consumer product or service.

As discussed in **section 3.4.1** of this chapter, consumers also need to be aware of non-monetary consideration, such as post-supply obligations of the consumer (including the provision of data and use restrictions).

While it is not new, this challenge can nevertheless be exacerbated by eObjects, because of their **dependency** and **use pattern**. This is particularly due to their common manifestation as product–service packages with more than one Provider.

Ascertaining payment terms may also be problematic, as may the consequences of a failure to pay, particularly when billing is done by more than one entity within the provider network. Payment terms, such as due dates and price increases, may vary greatly between one entity in the provider network and another. Any of the inhabitants of Everyware Place (**Vignette E1**) in the Vignettes may face this problem with the smart home installation in relation to the different devices and services that were made available through the initial set-up, and those that were added subsequently.

If consumers cannot easily ascertain the true price, this would conflict with the Consumer Goal of **Information**.

[790] See for example, *Australian Competition and Consumer Commission v AirAsia Berhad Co* [2012] FCA 1413; *Australian Competition and Consumer Commission v Jetstar Airways Pty Ltd (No 2)* [2017] FCA 205; *Australian Competition and Consumer Commission v Virgin Australian Airlines Pty Ltd (No 2)* [2017] FCA 204.

3.5.4 Liability allocation

Attributes and interactions: **Interactions with 1) living things, 2) the physical world, 3) other eObjects and 4) other computing devices and systems, Dependency**

Consumer Goals: **Redress**

As discussed in **Chapter 2**, eObjects can **interact** with living things, the physical world, other eObjects and/or other computing devices and systems. Often, eObjects **depend** on these interactions to operate. The complexity of these interactions, and the complexity of the contractual arrangements, both produce a significant challenge for consumers in establishing who is responsible for failure or loss. Defects in an eObject ecosystem causing detriment to consumers can arise in a number of different places. For example, physical faults in the dominant physical object, faults in the embedded computer hardware, bugs in the software, corruption or deletion of data, halts in service provision, or failure of network connections can all cause harm to consumers. The overall detriment may well arise from a combination of defects, including a network failure at a critical time that corrupts data, causing the eObject or the systems in which it participates to fail to recognise critical inputs and/or provide critical functionality.

If there is one Provider who has provided all of the hardware, software and associated services, then liability allocation is a relatively simple exercise. It is limited only by whether or not the particular type of loss is legitimately excluded under the contract. However, where there are multiple Providers providing goods and services, as is common, then the question becomes more complicated.

Failures in eObjects may result from different causes, which makes liability allocation more complicated, particularly questions of proof in discovering who is at fault. Environmental factors such as fire, flood and wind can cause direct damage, or indirectly cause a failure in an eObject or associated system, for example, by interrupting the power supply. Also, an eObject can stop working or have its functionality reduced by accident or unintentional error, such as a human cutting off a service in error, or a network

malfunction or other infrastructure failure. Deliberate attacks on eObjects may also cause problems for liability allocation.

For example, it will be difficult to track down the rogue who hacked into Jessica's house (**Vignette J5**) and caused the fire. If the rogue is based overseas, it is even less likely that law enforcement authorities will attempt to bring criminal proceedings against her/him in Australia. A consumer's real search for liability will begin with the provider network for the eObjects concerned. Jessica will first face the significant technical difficulty of isolating the main cause of the fire: that is, identifying that her smart home was in fact hacked, as opposed to being subject to some form of accident or environmental incident. The next question will be ascertaining from amongst the tens of Providers which of them could legally be held liable (which could be multiple Providers). Was it the developer of the lamp's software? Was it the designer of the security protections on the network? Was it the designer of the oven which failed to include an automatic switch-off functionality? A new set of uncertainties is likely to arise around concepts of causation and liability in contract law, under general consumer protection law, and in other areas such as tort and product liability law. Where entities from multiple jurisdictions are involved, with different rules as to allocation of liability, these uncertainties become even greater.

Challenges of liability allocation are not new, particular in areas where more than one supplier contributes to a product or service; nevertheless, the complexity of eObjects means that this challenge may manifest itself at a much greater scale than before. This challenge has a direct impact on the Consumer Goal of **Redress**. It is worth noting that is not only consumers who are concerned with allocation of liability, but all Providers. This type of uncertainty affects the industry as a whole. Uncertainty as to legal liability is likely to hinder investment and innovation in this emerging industry.[791]

[791] Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87) 18; European Commission, *A Digital Single Market Strategy for Europe COM (2015) 192 final* (2015), para 4.1.

3.5.5 Procedural issues

Attributes and interactions: **Core, mobility, portability**
Consumer Goals: **Redress**

Consumers who acquire digital content have always been subject to a wide range of commercial uncertainties in relation to dealing with businesses outside the consumer's jurisdiction. Website terms and conditions are commonly drafted to make an explicit choice of both governing law and the location of the jurisdiction in which any claims can be heard. Many, if not most, of the terms and conditions encountered by Australian consumers do not contain an Australian state in either the governing law clause or the jurisdiction clause. Therefore, many Australian consumers face significant logistical and financial challenges in making a claim if they are not located in the relevant Provider's jurisdiction, or if they are unfamiliar with the governing law of the contract.

This is not a *new* challenge facing those who buy eObjects, but rather one that is 'in common' with all online contracting. The legal issues are likely to be the same, although there may be some practical differences in bringing claims, and some increased uncertainty among consumers. The **mobility** and **portability** of eObjects may mean that jurisdictional and choice of law issues arise more often. Even when the eObjects themselves do not move between jurisdictions, these problems can arise. For instance, if the eObject or eObject ecosystem has a provider network with a number of diverse actors, some of these actors are likely to be based in different jurisdictions. The applicable contractual bundle may well mean that a consumer may be faced with the prospect of untangling clauses relating to multiple jurisdictions and multiple choices of law.[792] This will cause a significant impact on the Consumer Goal of **Redress**.

[792] Hon, Millard and Singh, 'Twenty Legal Considerations for Clouds of Things' (n 87) 8.

4 CONCLUDING REMARKS

This chapter has identified a number of challenges for consumers in consumer transactions arising out of new things, activities and relationships made possible by eObjects and eObject ecosystems. The challenges identified are those whose outcomes conflict with Consumer Goals expressed by the legislature and in the common law, in line with the approach set out in **sections 3** and **4** of **Chapter 3**. Due to this conflict, the challenges identified bear further investigation and analysis as to whether or not they are likely to give rise to legal problems. These challenges are not mere inconveniences to consumers. If they are not addressed, enforcement of the existing common law of contract and the ACL will not be sufficient to achieve the goals of consumer law agreed upon by federal and state governments in Australia.

However, it is important to remember that just because consumers may have challenges to face, this does not mean that legal problems exist (see discussion in **section 3** in **Chapter 3**). This is the case for two reasons. First, legislation or other rules may exist which have direct application to the new activities, things or relationships that cause consumers concern. Even where there are no decided cases that discuss that law's application to eObjects, an existing legal principle may still address the identified challenge.[793] In particular, contract and related consumer protection law in Australia is commonly drafted in broad terms, and is, at least to some extent, not technologically specific. This breadth and generality mean that in many cases existing principles may be applied by judges quite readily and satisfactorily to new circumstances, including activities, things and relationships made possible by eObjects. Second, consumers cannot legitimately expect legal protection from all challenges they might face. They have responsibilities as well as rights, such as a responsibility to inform themselves (to a reasonable extent) about the product they are buying.

[793] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 252–53.

The next logical step for further research would be to analyse the particular rules currently applicable to each challenge to ascertain the extent to which legal problems may arise. However, to do so for *every* challenge would be a colossal exercise, and impossible to undertake within the scope of this dissertation. **Section 3.3** of **Chapter 1** set out the rationale for a broad and deep approach to this research project. Following this rationale, the broad identification of a series of challenges for consumers undertaken in this chapter now gives way to an in-depth examination of *one* challenge. **Chapter 6** will provide a detailed doctrinal analysis of 'digital consumer manipulation' enabled by eObjects, the challenge outlined in **section 3.3.1** of **Chapter 5.** In particular, **Chapter 6** will investigate the extent to which regulatory disconnection has occurred or is likely to occur in the face of this type of sociotechnical change.

.

Chapter 6 – Digital consumer manipulation[794]

[794] This chapter reproduces substantial parts of a journal article published during the course of this doctoral study: Manwaring, 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (n 110). An earlier version of this article was presented at the British and Irish Law Education and Technology Association 2018 annual conference held at the University of Aberdeen on 10–11 April 2018. The paper was one of three shortlisted by a peer review panel and after an oral defence was voted by conference delegates as the winner of the 2018 Google Prize for best postgraduate paper.

1 AIMS OF CHAPTER

Chapter 5 identified a number of challenges for consumers in consumer transactions arising out of new things, activities and relationships made possible by the new sociotechnical landscape outlined in **Chapter 2**. As the outcomes of the identified challenges have the potential to conflict with the Consumer Goals set out in **section 4** of **Chapter 3**, they are all good candidates for further analysis as to the likelihood that they will give rise to regulatory disconnection, as discussed in **section 2.2.1.2** of **Chapter 3**.

However, to examine *all* of the challenges set out in **Chapter 5** would be impossible within the scope of this dissertation. Yet, the utility of the framework discussed in **Chapter 3** for uncovering legal problems in the face of sociotechnical change can be illustrated (at least in part) by examining one challenge. Therefore, in this chapter, the dissertation moves from its previously broad approach to an in-depth examination of one challenge, that of digital consumer manipulation, introduced in **section 3.3.1** of **Chapter 5**.

Digital consumer manipulation is examined in depth in this dissertation for a number of reasons. Apart from Calo's important 2014 work[795] relating to US law (discussed in **section 3.3.1** of **Chapter 5**), the topic has been under-researched by both legal scholars and policymakers. Until recently, very little attention had been paid to the additional threats posed by eObjects and related systems.[796] A lack of understanding of digital consumer manipulation undertaken through eObjects, and how Australian legal rules might apply to it, is problematic because so much of its nature (and disbenefits) is hidden from those it affects. Digital consumer manipulation activities are not advertised by companies other than in occasional vague references in privacy policies. The activities undertaken by companies, and their likely effects, are deliberately kept secret. If manipulative conduct is hidden from view, there is a significant possibility that behaviour which would be considered unacceptable by the majority of Australian citizens may escape the regulatory net.

To bring this issue some attention, the January 2016 research paper[797] by the author of this dissertation provided a preliminary review of the applicable consumer protection law and outlined the possibility of regulatory disconnection in relation to rules regarding misleading or deceptive conduct and unconscionable conduct in the ACL. In an article published later in 2016,[798] Mathews-Hunt also discussed the ACL provisions briefly in relation to online behavioural advertising (for conventional ecommerce, **not** mediated by eObjects), but stopped short of a detailed doctrinal analysis. Additional research relating to foreign jurisdictions was also published later in 2016 discussing problems relating to digital consumer manipulation in the

[795] Calo, 'Digital Market Manipulation' (n 42).

[796] However, see Calo's short magazine piece from 2013: Calo, 'Tiny Salespeople: Mediated Transactions and the Internet of Things' (n 105).

[797] Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (n 90). This paper was later revised and published as the journal article Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

[798] Mathews-Hunt, 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (n 56) 77–79.

context of both conventional ecommerce (under English law)[799] and some of the specific issues raised by eObjects (EU law).[800]

To properly fill the gap in the Australian context, this chapter provides a detailed doctrinal analysis of the areas of the ACL potentially dealing with digital consumer manipulation. This analysis is illustrated with the use of the Vignettes relating to Jessica and Fahim from **Chapter 4**.

The relevant legislative provisions contained in the ACL do not, on their face, suffer from a lack of technological neutrality (as discussed in **section 2.2.1.3** of **Chapter 3**). They are couched in very general terms, and as such, could form the basis of a claim relating to digital consumer manipulation. However, the doctrinal analysis in this chapter reveals that, in part due to the very generality of the terms, the operation of the current consumer law in this area is **uncertain**. This chapter concludes with a discussion of the nature of the uncertainty uncovered and its effect on regulatory timing, and proposes that greater specificity in rulemaking (whether legislative or judicial) can assist in dealing with sociotechnical change. However, the success of this proposal depends significantly on whether rule-making processes can be implemented that allow for a reasonably prompt reaction to sociotechnical change.

The chapter also examines the notion of corporate secrecy and proposes the possibility that in it lies a **new harm** that may affect consumers who buy and interact with eObjects. This arises from a lack of transparency in corporate dealings with consumer information.

This chapter does not examine all forms of digital consumer manipulation. The doctrinal analysis is confined to the particular, 'enhanced' forms of these practices in which eObjects are involved in data collection and/or delivery of marketing content. However, it is likely that some of the same arguments

[799] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42).

[800] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42).

might apply to digital consumer manipulation in the context of 'conventional' ecommerce. No Australian analysis of digital consumer manipulation has been located in the scholarly literature to date,[801] other than the article by the author of this dissertation on which this chapter is based.[802]

2 WHY IS DIGITAL CONSUMER MANIPULATION A CONCERN?

2.1 Consumer protection goals and the case of digital consumer manipulation

Section 3.3.1 of **Chapter 5** introduced the concept of 'digital consumer manipulation', its current and possible manifestations in relation to eObjects, and the potential for consumer detriment. **Vignettes F2**, **F4**, **J3**, **J9**, **J10**, **J11**, **J13** and **J14** provide examples of situations where consumers could be detrimentally affected by this type of marketing. As discussed in **Chapter 5**, where such manipulation is successful, it has the potential to undermine the Consumer Goals of **Fairness** and **Choice**, and in some cases that of **Disadvantage**.

So why does this matter? As pointed out in **section 3.3.1** of **Chapter 5**, persuasive tactics by advertisers are not new. Regulation or limitation of such tactics has always required something more egregious than mere persuasiveness. In the context of the Vignettes relating to Fahim and Jessica, marketers could respond to calls for regulation by saying 'there is nothing *forcing* Fahim or Jessica to make a purchase – they have a choice to go elsewhere or to not shop at all'. However, this argument ignores the

[801] However, see Mathews-Hunt, 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (n 56). This article does not deal directly with digital consumer manipulation, but some of the practices described and critiqued in this article are relevant to such conduct.

[802] Manwaring, 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (n 110).

important and complex question of whether the consumer actually does have a proper 'choice' in all circumstances of digital consumer manipulation.

A number of scholars have argued that choice[803] and autonomy[804] have significant and increasing potential to be impaired in a number of ways by digital consumer manipulation techniques. For example, Sax, Helberger and Bol[805] conducted an analysis of selling techniques used within mobile health applications (such as those used with fitness trackers and smartphones), and consumer responses to them. They concluded that these could lead to the undermining of autonomy in the following ways:

- alternative product and service options being obscured;
- unauthentic goals and desires being invoked in a consumer due to continued use of an application designed to be addictive[806] and/or the rewarding of behaviours desired by the supplier rather than those initially desired by the consumer;[807] and
- independent decision-making being circumvented due to the framing of economic choices as health or welfare choices.

Information asymmetry is 'a condition where … one party in a relationship has more or better information than another'.[808] Information asymmetry

[803] Maurice E Stucke and Ariel Ezrachi, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' (2017) 32 Berkeley Technology Law Journal 1239; Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42); Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42).

[804] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42); Calo, 'Digital Market Manipulation' (n 42); Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42).

[805] Marijn Sax, Natali Helberger and Nadine Bol, 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices' (2018) 41 Journal of Consumer Policy 103.

[806] See also Nir Eyal and Ryan Hoover, *Hooked: How to Build Habit-Forming Products* (Portfolio/Penguin 2014).

[807] See also Christl and Spiekermann, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (n 716) 61–62.

[808] Donald Bergh and others, 'Information Asymmetry in Management Research: Past Accomplishments and Future Opportunities' (2019) 45 Journal of Management 122, 123.

between supplier and consumer, which has long been seen as compromising consumer choice, is arguably increased by digital consumer manipulation.[809]

Other significant disbenefits of this type of conduct that have attracted condemnation include its potential to:

- be unfair to consumers;[810]
- violate privacy;[811]
- compromise the dignity of consumers;[812] and
- hinder or distort competition.[813]

It appears now that at least some regulatory agencies are coming to recognise the harms caused by this conduct. In March 2018, the European Data Protection Supervisor (**EDPS**) issued an Opinion concluding that '[o]nline manipulation poses a threat to society'.[814] Much of the EDPS's concern relates to the use of data collected by corporate and government actors to influence the outcome of elections. However, the EDPS also recognises the general undesirability of hidden manipulation of consumers and the possibility of harm arising out of breaches of privacy, hindrances to competition, and the encouragement of addictive behaviours (particularly in

[809] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 12–14.

[810] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 157; Calo, 'Digital Market Manipulation' (n 42) 237.

[811] Calo, 'Digital Market Manipulation' (n 42) 1027–31.

[812] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 154–55; Zarsky, 'Privacy and Manipulation in the Digital Age' (n 678) 175; Cass Sunstein, 'Fifty Shades of Manipulation' (2016) 1 Journal of Marketing Behaviour 213, 239.

[813] Stucke and Ezrachi, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' (n 803) 1256–70; Calo, 'Digital Market Manipulation' (n 42) 1026.

[814] European Data Protection Supervisor, Opinion 3/2018, EDPS Opinion on online manipulation and personal data (19 March 2018) 23. Harari also argues that we are currently seeing a 'shift in authority' to a concept he calls 'dataism'. As a result of this shift, the potential for harm to society may lie not only in manipulation by third parties, but in individuals themselves subjugating their own decision-making powers to those who have the ability to collect, control and analyse data: see Yuval Noah Harari and New Perspectives Quarterly, 'Dataism Is Our New God' (2017) 34 New Perspectives Quarterly 36; Yuval Noah Harari, *Homo Deus: A Brief History of Tomorrow* (Harvill Secker 2016).

children).[815] In December 2018, the ACCC released a report that acknowledged that commercial manipulation of consumers by means of eObjects 'present[ed] risks to the privacy and *autonomy* of users'.[816]

Increasing consumer unease with digital consumer manipulation practices, at least in relation to conventional ecommerce, is also a factor in considering regulation of digital consumer manipulation. The CPRC Survey in 2018 revealed that slightly over 50% of Australians surveyed found (conventional) targeted online advertising to be unacceptable, 27% found it acceptable, and around 20% were neutral.[817] This supports an earlier, very small[818] study of Australian users and developers of eObjects. This study included comments that users of eObjects 'were concerned about their personal data and others' ability to control and understand their patterns of behaviour stemming from their personal information'.[819] More generally, there was an expectation expressed by most consumers in the CPRC Survey that it was the responsibility of government to become involved in regulating how commercial entities use consumer data.[820] A 2016 review of US empirical

[815] European Data Protection Supervisor, *Opinion 3/2018, EDPS Opinion on online manipulation and personal data* 9, 10, 12.

[816] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* 328 (n 82) (emphasis added). The Council of Europe recently expressed a similar concern about the effects on the 'cognitive autonomy' of users and their right 'to take independent decisions': Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies) (Decl(13/02/2019)1).

[817] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) 61. The research question was 'How acceptable or unacceptable do you find it for companies to use your data in the following ways? Monitoring your online behaviour to show you relevant advertising and offers'. Of the respondents, 29.2% found this 'very unacceptable', 22.8% 'somewhat unacceptable', 19.8% 'neutral', 24.6 'somewhat acceptable' and 2.4% 'very acceptable'.

[818] Bosua and others, 'Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective' (n 102). This study contained 24 participants, 12 of whom were designers and users of eObjects, the other 12 just users.

[819] Ibid 9.

[820] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) 37. 73% of respondents indicated that

work on consumer attitudes to personalised targeting also found considerable disquiet amongst consumers faced with targeted advertising, although, like the Australian consumers surveyed, there was a range of attitudes.[821] There were some indications from the US data that consumers' actual marketplace activities were at odds with their expressed distaste for personalised advertising, as such advertising tended to be successful in increasing purchases.[822] However, this could be advanced as an argument against allowing these practices, as it implies that the techniques can be successful even when the consumer is aware of them and of the negative effects on their behaviour and interests. Forms of disclosure are frequently proposed to mitigate harmful effects on consumers, but these types of results provide some limited indication that disclosure is not effective.

All of these factors would suggest that digital consumer manipulation practices should be restricted in some way. However, it must be recognised that the line is sometimes difficult to draw between practices that are an acceptable part of competitive business practice, and those which unacceptably compromise consumer welfare.[823]

2.2 The changing situation of the consumer

This chapter argues that many digital consumer manipulation practices will not be prohibited, or even constrained, by the current consumer protection regime. Marketers have been exploiting the cognitive biases of consumers for many years through a number of means. What makes digital consumer manipulation different? In the context of digital consumer manipulation, this dissertation argues that the combination of 'intense systemati[s]ation

'[t]he Government should ensure companies give consumers options to opt out of what data they provide, how it can be used, and if it can be shared with others').

[821] Rena Coen and others, 'A User-Centered Perspective on Algorithmic Personalization' (Master of Information Management and Systems: Final Project, University of California, Berkeley, 6 May 2016) 10–11.

[822] Ibid.

[823] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 157.

and personali[s]ation'[824] innate in digital consumer manipulation, particularly when enhanced by eObjects, provides unprecedented opportunities for marketers when targeting such digital consumers. In other words, consumers have never before been in a position where:

1) suppliers know so much about individual consumers;
2) marketing analysts know so much about what combination of factors lead to particular purchase decisions;
3) marketing channels are so plentiful and diverse, and can target consumers in so many different places and at so many different times; and
4) consumers know very little about the rich variety of data that is collected, the inferences that may be drawn from it, and how those inferences might be exploited.[825]

To explain in practical terms how the changed position of the consumer affects marketing techniques, let us first look at an example of 'conventional' sales techniques. Jessica, 10 years ago, may have gone into her local shopping centre, as she does in **Vignettes J10–J12**. She would have moved through the centre and passed by a number of static ads. A decision to enter the pharmacy would mean that she would have passed through a fit-out and display designed to direct her steps past its most profitable products. An experienced salesperson would have been able to quickly and correctly peg her as a middle-aged working mother, time-poor but nevertheless looking for a bargain. The salesperson would have approached Jessica with suggestions based on her experience of previous similar customers' buying patterns, and with the types of compliments that are most likely to achieve a sale.

[824] Calo, 'Digital Market Manipulation' (n 42) 1021.

[825] Note, however, that consumer awareness may now be somewhat greater due to the publicity surrounding the Facebook data harvesting undertaken by Cambridge Analytica and related companies for the purposes of influencing the US presidential election and the Brexit referendum. See for example, Cadwalladr and Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' (n 104).

Compare the above situation to the Vignettes where Jessica's and Fahim's environments are 'enhanced' by eObjects. Max may have data on Jessica's digital purchases over the last two years, age, personality type, career, weight, household salary, physical activity, where she is at different times of the day and how often she visits particular places, what she eats, her relationships with families, friends and service providers, health, mood, and the day and time in the week when she is most likely to make a purchase. Fahim's and Jessica's phones collect data from other eObjects and conventional computers, and pass it on to third parties, such as the shopping centre. Jessica's television may well do something similar.[826] Marketing approaches are based on algorithms researched and developed by marketing experts with large budgets for behavioural research, heavily personalised to Jessica's and Fahim's profiles, and deliverable anytime and anywhere. The eObjects with which Jessica and Fahim interact adapt to the success or failure of particular marketing approaches, and add this to both Jessica's and Fahim's profiles and the profiles of other people like them.

Publicly available empirical research concerning the effectiveness of digital consumer manipulation using eObjects is scant.[827] However, it is arguable that seller persuasiveness is more likely to be effective because eObjects provide suppliers with more relevant information and new avenues to detect and capitalise on opportunities, and even create them, such that a consumer is highly likely to buy their product. Less obviously, the framing of offers and the immediacy of particular channels, such as an always-available digital personal assistant, or the convenience of a supplier-specific ordering button, are also relevant. These may reduce both the availability of information to the consumer and the scope for them to give it proper consideration.

[826] Andrew Laughlin, 'Which? Investigation Reveals "Staggering" Level of Smart Home Surveillance' (*Which?* 1 June 2018) <www.which.co.uk/news/2018/06/which-investigation-reveals-staggering-level-of-smart-home-surveillance> accessed 11 June 2018.

[827] However, one useful example of early-stage empirical research can be seen in Sax, Helberger and Bol, 'Health As a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices' (n 805).

3 LEGAL PROBLEMS IN AUSTRALIA ARISING FROM DIGITAL CONSUMER MANIPULATION USING eOBJECTS

3.1 How the ACL might deal with digital consumer manipulation

Digital consumer manipulation has been characterised by some scholars as a form of 'unfair persuasion'.[828] However, 'unfairness' is not recognised as a general principle of regulated conduct under the law in Australia (although note the discussion of unfair contract terms below). This contrasts with general prohibitions against unfair *commercial conduct* that can be found in other jurisdictions, such as in the US and Europe. For example, the US Federal Trade Commission Act[829] prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[830] Chapter 3 of the EU *Unfair Commercial Practices Directive*[831] prohibits '[u]nfair commercial practices' in general, and also provides a list in Annex I of specific practices that 'in all circumstances [would] be regarded as unfair'.[832] Claims arising out of digital consumer manipulation in the US and the EU are likely to invoke these prohibitions.[833] However, a detailed comparison of these prohibitions with the Australian law is beyond the scope of this dissertation.

Yet, a general prohibition on unfair conduct in commerce is not currently found in *Australian* law. Some *specific* sales techniques are designated as 'Unfair practices' in Part 3-1 of the ACL and regulated accordingly, namely:

- offering rebates, gifts and prizes (section 32 ACL);

[828] Calo, 'Digital Market Manipulation' (n 42) 1032. See also Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 157–58.

[829] 15 USC §§ 41–58.

[830] 15 USC § 45.

[831] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market [2005] OJ L149/22.

[832] This has been implemented, for example, in almost identical terms in The Consumer Protection from Unfair Trading Regulations 2008 (UK) reg 3.

[833] Calo, 'Digital Market Manipulation' (n 42); Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42).

- bait advertising (section 35 ACL);
- wrongfully accepting payment (section 36 ACL);
- providing unsolicited credit and debit cards (section 39 ACL) or other goods and services, including unauthorised advertising (sections 40–41 ACL); and
- pyramid selling (section 44 ACL).

False and misleading representations are also included as 'Unfair practices' under section 29 in Part 3-1 of the ACL, but this section is dealt with separately below. However, none of the provisions in Part 3-1 listed above (save for section 29) apply generally to digital consumer manipulation techniques (although such techniques could be used to carry out regulated conduct, such as a service provider using Max in **Vignette J3** for bait advertising). However, the ACL *as a whole* (and its predecessor statute, the Trade Practices Act 1974 (Cth) (**TPA**)) does not exclude digital consumers, nor attempts to manipulate them. Some *general* principles are contained in the ACL that judges can call upon to restrict the ways Providers might manipulate digital consumers into forming contracts, most importantly in provisions regulating misleading, deceptive and/or unconscionable conduct.

As discussed above, suppliers will usually be in a position to know much more about their products or services than consumers, and the provision of false or misleading information can affect individual choice and competition. The ACL attempts to enable '*informed* commercial activity'[834] by prohibiting suppliers providing false, misleading and/or deceptive information to consumers about their products and services. Therefore, **section 3.2** of this chapter discusses the potential application to digital consumer manipulation of the general legislative provisions prohibiting misleading or deceptive conduct (section 18 ACL), and specific false and misleading representations (section 29 ACL). This chapter does not deal with common law misrepresentation as it has a narrower application and less effective remedies than the ACL provisions in the business-to-consumer context.[835] However,

[834] *Bullabidgee Pty Ltd v McCleary* [2011] NSWCA 259 [69] (emphasis added).

[835] Dilan Thampapillai, Claudio Bozzi and Alex Bruce, *Contract Law: Text and Cases* (2nd edn, LexisNexis Butterworths 2016) 510.

this chapter concludes that some digital consumer manipulation may fall outside the prohibitions, even if it is otherwise objectionable or unfair.

Misleading or deceptive conduct may lead to significant information asymmetry, to the disbenefit of consumers and their decision-making processes. However, it has long been recognised in both case and statute law that consumers' decision-making processes can be manipulated in other ways, such as where one party suffers from a disadvantage and the other exploits that advantage to the first party's detriment.[836] Therefore, **section 3.3** of this chapter discusses the application of statutory (and, where relevant, equitable) principles relating to unconscionable conduct (sections 21–22 ACL) to digital consumer manipulation. Unfortunately, this chapter concludes that there are some significant barriers to using unconscionable conduct principles to regulate unwanted forms of digital consumer manipulation.

Section 3.5 of this chapter will also briefly discuss the potential relevance of other areas of law, such as ACL provisions regulating unsolicited consumer agreements (ACL, Part 3-2, Div 2); other legislative provisions regarding privacy and spam; and the doctrines of duress, undue influence and mistake. It does **not** consider the effect of the unfair contract terms regime contained in Part 2-3 of the ACL, as this regime excludes terms relating to subject matter and price,[837] which are usually the most prominent in deciding whether to enter into a consumer contract. Nor does this chapter consider the Contracts Review Act 1980 (NSW) (**CRA**), which provides relief against unjust, harsh or oppressive contracts or contractual terms,[838] because it is limited to contracts for which the law of New South Wales (**NSW**) is the proper law of the contract.[839] Of course, if digital consumer manipulation does result in a contract that contains unfair terms covered by Part 2-3 of the

[836] For example, *Commercial Bank of Australia Ltd v Amadio* [1983] HCA 14 (*Amadio*).
[837] ACL s 26.
[838] Contracts Review Act 1980 (NSW) ss 4, 7, 8, sch 1.
[839] Ibid s 17.

ACL, then a consideration of that part would be relevant. The same applies to the CRA if NSW is the proper law of the resulting contract.

3.2 Misleading or deceptive conduct

3.2.1 Elements of misleading or deceptive conduct; false or misleading representations

Marketing practices must comply with the ACL provisions prohibiting 'misleading or deceptive conduct' (section 18 ACL) and 'false or misleading representations' (section 29 ACL). While section 18 applies generally, section 29 prohibits a set of *specific* false and misleading representations from a 'closed list' regarding supply and promotion of goods and services, including misrepresentations relating to price (section 29(1)(i)), quality (section 29(1)(a)–(b)), performance characteristics or uses (section 29(1)(g)), place of origin (section 29(1)(k)), necessity (section 29(1)(l)), and sponsorship (sections 29(1)(g)–(h)). Mirror provisions relating to financial services are found in sections 12DA and 12DB of the Australian Securities and Investments Commission Act 2001 (Cth) (**ASIC Act**). The ASIC Act provisions are relevant in two ways. First, the cases on the mirror provisions are relevant as precedents for ACL cases (and vice versa). Second, eObjects can be used to provide financial services and therefore the ASIC Act can be directly applicable.

The integers underlying both sections are set out in **Table 7**:

Table 7: Comparison of sections 18 and 29 ACL

	Section 18 prohibits:	**Section 29 prohibits:**
1	A person	Same
2	In trade or commerce	Same
3	Engaging in conduct	Representation (closed list)
4	Which is misleading or deceptive	False or misleading
5	Or is likely to mislead or deceive	No
6		In connection with the supply/possible supply/promotion of goods/services

Integers 1 and 2 of section 18 are repeated in section 29, but what is prohibited is 'false or misleading representations'. For integer 4, it is unlikely that anything substantial turns on the difference in terminology. There is a view that 'deceptive' *may* have a narrower meaning than 'misleading', but this is relatively unexplored,[840] and Australian judges have tended to treat the terms 'false or misleading' in section 29 synonymously with the terms 'misleading or deceptive' in section 18.[841] However, there are five significant differences between sections 18 and 29:

1) (integer 3) the requirement in section 29 of 'representations' which is narrower than the 'conduct' prohibited in section 18;
2) (integer 3) the closed list of representations prohibited by section 29, as opposed to the open definition of conduct regulated in section 18;
3) (integer 5) the inclusion of 'likely to' in section 18;

[840] Colin Lockhart, *The Law of Misleading or Deceptive Conduct* (5th edn, LexisNexis Butterworths 2019) [3.2] 89–90, fns 13, 14.

[841] *Australian Competition and Consumer Commission v Dukemaster Pty Ltd* [2009] FCA 682 (*Dukemaster*); *Australian Competition and Consumer Commission v Coles Supermarkets Australia Pty Ltd* [2014] FCA 634; *Comite Interprofessionel du Vin de Champagne v Powell* [2015] FCA 110.

4) (integer 6) the required connection with the supply/promotion of goods/services in section 29; and
5) the type of remedies applicable, as section 18 remedies are substantially confined to the civil remedies available under the ACL (such as damages/compensation orders, injunctions, orders for contract variation or rescission, and adverse publicity orders)[842] while a breach of section 29 can additionally attract civil pecuniary penalties[843] and criminal remedies.[844]
6) Integers 1 and 2 of sections 18 and 29 are the same, and easily satisfied in relation to digital consumer manipulation.

In relation to integer 3, section 29 requires a *representation*, that is, a 'statement, made orally or in writing or by implication from words or conduct, relating to a matter of fact'.[845] If the representation is false or misleading in relation to one of the elements of the closed list, then it is an actionable misrepresentation under the section. However, modern cases have made it clear that the section 18 term 'conduct' is wider than a section 29 'representation'.[846] Not only does it cover conduct outside the closed list, it also prohibits both misrepresentations and other forms of conduct. In *Butcher v Lachlan Elder Realty Pty Ltd* (*Butcher*)[847] the High Court rejected earlier contentions that section 18 (then section 52 of the TPA) required a misrepresentation.[848] In this case all the judges held that the term 'conduct' in the section extended *beyond* representations. In 2010, the

[842] ACL: s 236 (damages), s 237 (compensation), ss 232–35 (injunctions), s 247 (adverse publicity orders), s 243 (variation or rescission of contract). This list is not exhaustive. Other orders are available under ACL ch 5.

[843] ACL ss 224–31.

[844] ACL s 151.

[845] Russell V Miller, *Miller's Australian Competition and Consumer Law Annotated* (Thomson Reuters 2016) 1670. See also *Given v Pryor* (1979) 39 FLR 437; *Aqua-Marine Marketing Pty Ltd v Pacific Reef Fisheries (Australia) Pty Ltd (No 5)* [2012] FCA 908.

[846] For a wide-ranging discussion of the case law on this point, see Alex Bruce, *Consumer Protection Law in Australia* (2nd edn, LexisNexis Butterworths 2014) 85–86.

[847] [2004] HCA 60.

[848] *Butcher v Lachlan Elder Realty Pty Ltd* [2004] HCA 60 (*Butcher*) [32], [103]. See also *Campbell v Backoffice Investments Pty Ltd* [2009] HCA 25 (*Campbell v Backoffice*).

High Court confirmed that '[f]or conduct to be misleading or deceptive it is not necessary that it convey express or implied representations … It suffices that it leads or is likely to lead into error'.[849]

The difference in integer 6 is unlikely to make any difference in the context of digital consumer manipulation. However, the same cannot be said for integer 5. The High Court has made it clear that if conduct is only required to be 'likely to' mislead or deceive, then there is no need to prove anyone was *actually* deceived or misled.[850] The conduct must just be *capable* of misleading or deceiving someone, to the extent there is a 'real or not remote chance or possibility'.[851]

The meaning of misleading or deceptive conduct in practice has been the subject of a rich variety of case law. However, the case law has made it clear that what constitutes misleading or deceptive conduct will depend on all of the circumstances of the case. Gordon J in *Dukemaster*[852] helpfully summarised a series of principles developed by courts relating to conduct regulated under section 18 (then section 52 of the TPA). The principles relevant to digital consumer manipulation techniques are:

> 1. … The 'conduct', in the circumstances, must lead, or be capable of leading, a person into error … and the error or misconception must result from 'conduct' of the corporation and not from other circumstances for which the corporation is not responsible …
>
> 2. … [the section] is concerned with the effect or likely effect of 'conduct' upon the minds of that person or those persons in relation to whom the question of whether the 'conduct' is or is likely to be

[849] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Ltd* (*Miller*) [2010] HCA 31 [15].

[850] *Google Inc v Australian Competition and Consumer Commission* [2013] HCA 1 [6]. See also *Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd* [1982] HCA 44 (*Parkdale v Puxu*) [8]; *McWilliams Wines Pty Ltd v McDonald's System of Australia Ltd* [1980] FCA 188, 411.

[851] *Dukemaster* (n 841) [10]. See also *Global Sportsman Pty Ltd v Mirror Newspapers Ltd* [1984] FCA 180 (*Global Sportsman v Mirror Newspapers*) [87].

[852] *Dukemaster* (n 841).

> misleading or deceptive falls to be tested. The test is objective and the Court must determine the question for itself …
>
> 3 … [the section] … is not designed for the benefit of persons who fail, in the circumstances of the case, to take reasonable care of their own interests …[853]

To properly analyse the law in relation to digital consumer manipulation, it is important to understand concepts relevant to sections 18 and 29, particularly the nature of 'conduct', the meaning of 'leading into error' and the extent to which consumers must take 'reasonable care of their own interests' in assessing the effect or likely effect of conduct. These elements are discussed in **sections 3.2.2**, **3.2.3,** and **3.2.4** of this chapter.

3.2.2 Conduct and misrepresentations

The differences between 'representations' required by section 29 and 'conduct' in section 18 may matter in some cases of digital consumer manipulation. This is because some techniques otherwise falling within section 29's closed list will arguably not amount to misrepresentations. For example, the sales technique of personalised pricing – where the price of an offer is calculated based on collected data about an individual's willingness to pay – is not dependent upon a misrepresentation. Nevertheless, it could be considered unfair and manipulative, as discussed below.

For example, in **Vignette J13**, Jessica is manipulated into paying an inflated price to buy her sister flowers. The Provider supporting Max's search and ordering services has had the opportunity to build a detailed personalised profile of Jessica, including the timing of her sibling's birthday, the nature of her recent interactions, and previous information on her willingness to pay in particular situations. If the 'exigency mark-up' imposed in this instance is shared between the company that provides Jessica with Max and the florist, both have incentives to raise the price to close to the limit that the available data suggests that Jessica will pay.

[853] Ibid [10].

Variable, personalised or dynamic pricing is not generally prohibited. In Australia, personalised pricing is available at weekend markets and car dealerships. Supermarkets offer the same goods at different prices based on the location of the store. Prices based on willingness to pay are readily available on auction websites. However, it is worth noting that there is evidence that many consumers find variable pricing practices unfair. The CPRC Survey found that 88% of consumers found it unacceptable to '[c]harg[e] people different prices for the same products in the same hour, based on their past purchasing, online browsing history, or payment behaviour'.[854]

There has been some regulator activity relating to one form of variable pricing: demand-based pricing. In 2016, the ACCC issued guidance to businesses on complying with the ACL regarding algorithmically generated dynamic pricing based on market demand.[855] This is commonly offered by businesses operating online 'sharing economy' platforms (such as surge pricing by car hire service Uber).[856] The regulator took no issue with the legality of the practice itself. The ACCC merely warned platform operators against saying their prices were lower than their competitors if the algorithmic pricing made this false in some instances. It also warned platform providers that if they had told their clients their pricing was demand-based, price increases for reasons other than demand would be misleading.

Misrepresentations relating to price are prohibited by section 29(1)(i) of the ACL. However, no misrepresentation is identifiable in **Vignette J13** described above. The service provider has programmed Max to 'take advantage' of consumers in exigent situations by increasing the price. However, absent a

[854] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) 61 (76.9% of consumers found it 'very unacceptable' and 11.2% of consumers found it 'somewhat unacceptable').

[855] Australian Competition and Consumer Commission, *Platform Operators in the Sharing Economy: A Guide for Complying with the Competition and Consumer Law in Australia* (3 November 2016).

[856] Uber, 'What is Surge?' <https://help.uber.com/h/e9375d5e-917b-4bc5-8142-23b89a440eec> accessed 9 September 2018.

misrepresentation that, for example, pricing is 'commission-free', this would not constitute a breach of section 29(1)(i). The relevant question would then be whether, in the absence of such a misrepresentation, the conduct of imposing an 'exigency mark-up' without the knowledge of the customer would constitute a breach of section 18. This situation is discussed further in **section 3.2.4** of this chapter.

3.2.3 'Leading into error': factual errors versus evaluative errors

As discussed in **section 3.2.1** of this chapter, section 18 of the ACL covers a broader range of conduct than section 29. This is due to its open-ended definition and the absence of a misrepresentation requirement. However, even absent a misrepresentation, someone must be led (or likely to be led) into error.[857] Problems may arise depending on how judges interpret this requirement when faced with digital consumer manipulation techniques.

Applying the section to digital consumer manipulation is problematic due to the nature of the type of 'error' required. Craswell[858] helpfully summarised several approaches generally used by advertisers to influence customers. First, advertising may act to change a consumer's *factual* belief about a product, such as comparative price or quality. Second, advertising may change a consumer's *decision-making processes* about whether to buy a product. Third, advertising can influence customers by producing a 'fundamental liking or disliking for a brand that cannot be explained … as resulting from specific beliefs about particular attributes', such as might happen when a product is continually associated with a favourable image.[859] Craswell considered '[t]he key distinction is that false factual beliefs represent errors of *fact*, while other forms of influence represent errors, if they can be called that, of *evaluation* or of *normative judgment*'.[860]

[857] *Miller* (n 849) [15].

[858] Richard Craswell, 'Interpreting Deceptive Advertising' (1985) 65 Boston University Law Review 657.

[859] Ibid 662–63.

[860] Ibid 665 (emphasis added).

One concern about digital consumer manipulation is that, if successful, it is much more likely to lead to consumer 'errors' falling into the latter category, a category this dissertation calls 'evaluative errors'. For example, in **Vignette J9**, if Jessica is convinced by the techniques employed that she should hide her wrinkles and split ends to be successful in her business, then this is likely to constitute an evaluative error. The error may only be made once, or a number of times, particularly if Max is programmed to give follow-up compliments or other nudges to operate upon Jessica's cognitive biases or discovered decision-making triggers.

However, the Australian judgments are focused on the existence or possibility of a *factual* error, rather than the *evaluative error*s brought about by an advertiser's *influence* on decision-making processes or fundamental attitudes towards brands.

Despite the High Court's pronouncements in *Butcher*, *Campbell v Backoffice* and *Miller* (discussed in **section 3.2.1** of this chapter) that section 18 requires 'conduct' rather than a 'misrepresentation', most successful Australian claims under the section are based on some form of false or misleading statement of fact.[861] These clearly fall into Craswell's 'factual error' category. Some cases have been successful which do *not* involve such a misrepresentation. But 'almost invariably the claim will focus on specific acts or omissions', rather than a claim that everything the defendant has done has been misleading or deceptive.[862] Common acts or omissions that do not involve a traditional misrepresentation have included silence, opinions, statements as to future matters, statements of law and unauthorised use of character images.[863] This cannot be a closed list given the High Court statements and the statutory language relating generally to 'conduct'. However, the decided 'non-misrepresentation' cases can be characterised as ones in which consumers

[861] JD Heydon, *Trade Practices Law: Competition and Consumer Law* (Thomson Legal & Regulatory) [160.430] (online version, accessed 7 August 2018).

[862] Stephen G Corones, *The Australian Consumer Law* (3rd edn, Lawbook Co 2016) [3.18].

[863] Colin Lockhart, *The Law of Misleading or Deceptive Conduct* (4th edn, LexisNexis Butterworths 2015) [2.5]–[2.6]; Heydon, *Trade Practices Law: Competition and Consumer Law* (n 861) [160.430] (accessed 16 January 2018).

were led into a factual error in the Craswell sense, and not an evaluative error.

For example, in the silence cases, victims were led into the factual error that all material facts *had* been disclosed. In the cases of opinion and statements as to future matters, the consumer's factual error was that the opinion was based on reasonable grounds. Regarding unauthorised use of character images, judicial reasoning has focussed on the factual error that the owner of the intellectual property rights in the image has consented to their use for that particular purpose.[864] Although it is common to make a distinction between statements of fact and statements of law, a misleading statement of the law still contains a factual error in the Craswell sense: the factual error subsists in the mistaken belief that a particular principle can be enforced by legal means when in fact it cannot (and vice versa).[865]

Max's comment in **Vignette J14** that its recommended smartphone contract is the one that 'best suits [Jessica's] likely needs' brings up interesting questions of proof. Section 4 of the ACL states that any representation as to a future matter must be based on 'reasonable grounds'; otherwise it is misleading. Case law has established that statements of opinion must be genuinely held; if they are not, they can be misleading.[866] Some eObjects can make decisions with high levels of **autonomy**, based on technologies with emergent properties: that is, properties that cannot be fully understood by humans.[867] In such cases, proof that an opinion is genuinely held, or that a statement about the future is based on reasonable grounds, may be difficult to produce, particularly with highly personalised recommendations and

[864] For example, *Pacific Dunlop Ltd v Hogan* [1989] FCA 185.

[865] *Public Trustee v Taylor* [1978] VR 289.

[866] *Tobacco Institute of Australia Ltd v Australian Federation of Consumer Organisations Inc* [1992] FCA 630 [47]; *Global Sportsman v Mirror Newspapers* (n 851) [17]; *Commonwealth Bank of Australia v Smith* [1991] FCA 375 [71]–[72]; *Stoker v Pomcol Pty Ltd* [1987] FCA 90 [15]; *Adour Holdings Pty Ltd v Commonwealth Bank of Australia* [1991] FCA 502 [21].

[867] Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (n 624) 10.

those based on autonomous technological agents. This may cause problems for the Provider/s responsible for Max's services. If Jessica or the ACCC can lead evidence that the smartphone contract was not very advantageous to Jessica, the burden of proof will most likely shift to Max's service provider.[868]

3.2.4 'Effect or likely effect on conduct' and 'reasonable care'

As stated by the Full Federal Court in *Global Sportsman v Mirror Newspapers*, the court must be 'concerned with the effect or likely effect of conduct upon the minds of those by reference to whom the question of whether the conduct is or is likely to be misleading or deceptive falls to be tested'.[869] The test as to whether such conduct was misleading or deceptive is an objective rather than a subjective one.[870]

In the context of digital consumer manipulation, there are two questions of concern when assessing the effect or likely effect of the conduct at issue (that is, whether it misled or deceived, or was likely to):

1) Who is the target audience?[871] and
2) What 'standard of skill and care'[872] is required of that audience?

The 'target audience' for most forms of advertising is considered to be the public as a whole or a particular segment of the public. For example, in *Australian Competition and Consumer Commission v TPG Internet Pty Ltd*,[873] where the allegations of misleading or deceptive conduct pertained to a multi-media advertising campaign offering an ADSL2+[874] service, the

[868] *Noone v Operation Smile (Australia) Inc* [2012] VSCA 91; 38 VR 569 [78].

[869] *Global Sportsman v Mirror Newspapers* (n 851) [14].

[870] Ibid.

[871] *Taco Co of Australia Inc v Taco Bell Pty Ltd* (1982) 42 ALR 177 (*Taco Bell*) 181; *Weitmann v Katies Ltd* (1977) 29 FLR 336, 339–40; *Brock v Terrace Times Pty Ltd* (1982) ATPR 40-267, [43412].

[872] Lockhart, *The Law of Misleading or Deceptive Conduct* (n 863) [3.25].

[873] *Australian Competition and Consumer Commission v TPG Internet Pty Ltd* [2013] HCA 54.

[874] ADSL is an Asymmetric Digital Subscriber Line service. At the time, ASDL2+ was considered to be a high-speed version.

relevant audience was held to be that segment of the public that was in the market for broadband services. For *personalised* advertising, as is the case with most digital consumer manipulation activities, the 'audience' would arguably be characterised as the *individual* target of the advertising, although this has not been tested. However, this may not always be the case. Some forms of personalised advertising are carried out without the advertiser knowing the 'individual' they are targeting. For example, de-identified data is used by marketers and data brokers[875] to create anonymised groups, which can then be served targeted advertising based on individual preferences or circumstances. This advertising can be achieved without the relevant advertiser ever having access to information about an 'identified' individual.[876] Rather it can serve up specific ads to individuals within a targeted group: for example, females aged 40–55 years with children of primary school age, a history of shoe purchases at a certain frequency, and currently within 5 metres of a dynamic advertising screen (where the ad can be displayed) in a Westfield shopping centre located in metropolitan Sydney.

The standard of care expected of the target audience varies with the objective characteristics of the audience, including its size.[877] For the public at large, or a segment of the public, there has also been a significant variance in approaches. Some UK statements based on the law of passing off have been quite broad, for example including all persons in the target audience other than 'moron[s] in a hurry'.[878] Early Australian formulations included:

[875] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (n 645) 27–29.

[876] See for example, Ariel Bogle, 'I Asked Everyone from Facebook to Data Brokers to Stan for My Information. It Got Messy' (*ABC Radio Australia,* 28 April 2018) <www.radioaustralia.net.au/international/2018-04-28/i-asked-everyone-from-facebook-to-data-brokers-to-stan-for-my-information-it-got-messy/1752610> accessed 28 April 2018.

[877] Lockhart, *The Law of Misleading or Deceptive Conduct* (n 863) [3.25]–[3.29]. See also *Campomar Sociedad Limitada v Nike International Ltd* [2000] HCA 12 (*Campomar*) [103]; *Taco Bell* (n 871) 202.

[878] *Morning Star Co-op Society Ltd v Express Newspapers Ltd* (1978) 1A IPR 661, 664.

> the effect on a person, not particularly intelligent or well informed, but perhaps of somewhat less than average intelligence, although the test is not the effect on a person who is, for example, quite unusually stupid.[879]

This test is sometimes still quoted, at least by trial judges.[880] However, the test, particularly as used in the High Court, has also been the subject of narrower formulations. Gibbs CJ in *Parkdale v Puxu* considered that the relevant question was:

> the effect of the conduct on reasonable members of the class. The heavy burdens which the section creates cannot have been intended to be imposed for the benefit of persons who fail to take reasonable care of their own interest.[881]

The 'reasonable care' standard has been supported in a number of subsequent cases.[882] The High Court in *Campomar* held the relevant question to ask is whether 'the "ordinary" or "reasonable" members of the class of prospective purchasers of a mass marketed product for general use'[883] would be misled, and the court could exclude the effect of those 'whose reactions are extreme or fanciful'.[884] However, the difference between an 'ordinary' consumer and a 'reasonable' one is still unclear. More recently, the High Court in *ACCC v TPG*[885] also adopted the *Parkdale v Puxu* formulation of

[879] *Annand & Thompson Pty Ltd v Trade Practices Commission* [1979] FCA 62 [26].

[880] For example, *Guy v Crown Melbourne Ltd (No 2)* [2018] FCA 36 (*Guy v Crown*) [330].

[881] *Parkdale v Puxu* (n 850) [9].

[882] *Commercial Dynamics Pty Ltd v M Hawke Nominees Pty Ltd* [1996] FCA 1394 [8]; *WEA International Inc v Hanimex Corp Ltd* [1987] FCA 379 [22]; *Tec & Tomas (Australia) Pty Ltd v Matsumiya Computer Co Pty Ltd* [1984] FCA 14 [25]; *Decor Corp Pty Ltd v BoWater Scott Ltd* [1985] FCA 218 [15], [17]; *National Exchange Pty Ltd v Australian Securities & Investments Commission* [2004] FCAFC 90 (*National Exchange v ASIC*) [18].

[883] *Campomar* (n 877) [105].

[884] Ibid.

[885] *ACCC v TPG* (n 873).

'reasonable care'. However, it was subject to the qualification of a causal link connecting the defendant's conduct and the error of the alleged victim.[886]

However, in *Taco Bell*[887] and *Butcher*[888] the Federal Court and the High Court, respectively, indicated that a different approach should be used when the target audience was 'identified individuals' rather than the public or a member of the public. Further to this, the High Court in *Butcher* stated that when individual consumers seek specific redress such as damages, two criteria must be met. First, '[t]he plaintiff must establish a causal link between the impugned conduct and the loss that is claimed.'[889] Second, the court must consider the subjective knowledge of both parties, including:

> the character of the particular conduct of the particular agent in relation to the particular purchasers, bearing in mind what matters of fact each knew about the other as a result of the nature of their dealings and the conversations between them, or which each may be taken to have known.[890]

In the context of digital consumer manipulation, application of the principle above would appear to imply that judges can and should consider the enhanced knowledge marketers can gain about individuals using the data collection techniques made possible by eObjects. The High Court, however, went on to hold that the assessment must continue by reference to what 'a reasonable person in the position of the [alleged victim], taking into account what they knew, would make of the [alleged perpetrator's] behaviour'.[891]

However, Lockhart casts some doubt on the existing authority that this requirement of a 'reasonable person' applies in all cases.[892] He proposes instead that *Butcher* and subsequent cases were only intended to apply to

[886] Ibid [39].
[887] *Taco Bell* (n 871).
[888] *Butcher* (n 848).
[889] Ibid [37].
[890] Ibid.
[891] Ibid [50].
[892] Lockhart, *The Law of Misleading or Deceptive Conduct* (n 863) [3.29].

relatively sophisticated purchasers and high-value property, where a greater standard of care should be expected. His assessment of the interpretation of the 'reasonable care' standard in the High Court and lower courts is that 'extreme, fanciful or unusually foolish interpretations of widely disseminated conduct' will mean that the relevant sections are not breached, but 'uncertainty remains' as the extent to which a 'reasonable care' standard can be applied.[893]

If a criterion of 'reasonable care' *is* applied, this is problematic for at least some digital consumer manipulation cases. If the relevant conduct is intended to exploit cognitive biases, it is intended to undermine the consumer's very capacity to take such reasonable care. This renders the test insufficient to achieve the goals of the ACL. The focus of digital consumer manipulation techniques is to convert an ordinary 'reasonable' consumer into a vulnerable one,[894] in the sense that they are less likely to exercise reasonable care in making a decision to buy a supplier's product or service. Marketers attempt to undertake this conversion in two stages. First, they undertake personalised data collection programs to discover what particular weaknesses and cognitive biases operate most strongly within particular individuals. For example, in 2017, access to databases containing contact details of 'wheelchair and insulin users, of people addicted to alcohol, drugs, and gambling, as well as … suffering from breast cancer, HIV, clinical depression, impotence, and vaginal infections' were offered on a commercial basis.[895] Then, they find opportunities to exploit those weaknesses and biases in individuals, based on behavioural research. For example, in 2013, a US marketing firm released a study claiming to identify the day and times of the week when women 'feel their least attractive', and then recommended a

[893] Ibid.

[894] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42) 160.

[895] Christl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (n 649) 39; DMDatabases, 'Ailments Mailing Lists/Email Lists' <http://dmdatabases.com/databases/consumer-mailing-lists/ailments-lists> accessed 30 June 2018.

strategy to beauty product marketers 'to heavy-up and wrap marketing … activity around the days that the beauty consumer feels the best and worst about her image'.[896] It is not new that commercial entities hold and use large amounts of consumer data. What is new and is occurring at an unprecedented scale is the intensity and extensiveness of the collection, the sophistication of the processing, the degree of automation, and the social distance of marketer from customer. Further, the combination of these aspects and the scale at which they operate, compounds the impact on the balance between seller and buyer.

An example of this can be found in **Vignettes F4** and **J9–J14** where Jessica and Fahim are the subjects of manipulative techniques designed to persuade them to buy consumer products. Each of Jessica and Fahim's data profiles has been used to target them at a time and place designed to minimise resistance to entering into a transaction.

These techniques are not scattergun approaches designed to pull in as many consumers as possible, such as those used by physical posters in a food court, or television ads; they are personalised to each of Jessica and Fahim, or at least people with characteristics very like them. Fahim has been targeted based upon time, location and his earlier purchasing patterns. Jessica's manipulation by beauty product marketers is somewhat more sophisticated, consisting as it does of:

1) identification of a possible vulnerability by surveillance of her comments to Max and the hairbrush's use as data collector and signaller;
2) embedding of vulnerability by the targeted storytelling ad on the electronic billboard in the shopping centre; and
3) further pressure to purchase due to the location- and time-targeted discount.

[896] PHDmedia, 'New Beauty Study Reveals Days, Times and Occasions When US Women Feel Least Attractive' (*Cision PR Newswire*, 2 October 2013) <www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html> accessed 1 January 2016.

Even more intimate data might also be used, such as that derived from menstrual cycle tracking applications on smartphones or wearables.[897] Some or all of these levels of manipulation might be considered *unfair*, in that they involve a business taking advantage of a vulnerable consumer.[898] However, this dissertation argues that the manipulation is not on its face *misleading* or *deceptive*. It therefore falls outside the scope of the prohibitions contained in sections 18 and 29 of the ACL. For this reason, the imposition of the exigency mark-up on flowers for Jessica's sister (discussed above at **section 3.2.2** of this chapter) is also unlikely to breach section 18. Merely unfair or distasteful conduct does not constitute a breach of either section 18 or indeed section 29.

3.2.5 Conclusion

Where digital consumer manipulation involves a misrepresentation, sections 18 and 29 of the ACL will apply to such conduct. Where the conduct does not amount to a representation, section 18 will only apply where the consumer is led (or likely to be led) into a factual error. If the error is an evaluative one, such as where the consumer's biases are exploited to an extent that their actions are considered not 'reasonable', then the sections will not apply. In these circumstances, Providers are not giving the consumer incorrect or incomplete information as to any innate attribute of the goods or services. Rather, consumers are being put in a situation where they are more likely to agree to buy the goods or services due to their own vulnerabilities, which is Jessica's, Mylin's and Fahim's situation outlined in **Vignettes J12**, **J13** and **F4**.

The analysis above shows that digital consumer manipulation techniques are not wholly unregulated by the existing law. Where such techniques lead consumers into a factual error (as defined in **section 3.2.3** of this chapter),

[897] Garmin, 'Menstrual cycle tracking' <https://connect.garmin.com/features/menstrual-cycle-tracking/> accessed 9 May 2019.

[898] Gerard Brody and Katherine Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (2016) 41 Alternative Law Journal 169, 169.

they will infringe the ACL provisions on misleading or deceptive conduct and specific misrepresentations. However, sanctions arising under these provisions are commonly triggered when the relevant conduct produces or is likely to produce a detrimental effect on the 'reasonable consumer'. In cases where there is no factual 'error', but the techniques nevertheless create a vulnerability to the extent that consumers are persuaded to act unlike 'reasonable' or 'ordinary' consumers, these provisions will not provide protection to consumers from digital consumer manipulation.

One suggested way to address the problem of 'information asymmetry' (identified in **section 2.1** of this chapter) is to consider shifting the general burden of proof from the regulator or consumer to the defendant.[899] However, this would not aid in the overall applicability of section 18 and/or section 29 to digital consumer manipulation. The target of the sections is not *manipulative* conduct by advertisers, but rather *misleading or deceptive* conduct. Advertisers may mislead or deceive in order to manipulate, but this is not *necessary*. If manipulation emanates from other forms of conduct, then the sections will simply not apply.

The ability of consumers to protect themselves may well improve over time, once consumers become more aware (and therefore warier) of these practices. Digital literacy programs in schools discussing digital marketing practices may assist to increase this awareness. However, a growth in understanding is likely to be hindered by the lack of incentive, or real disincentive, for service providers to reveal details of these practices. Corporate secrecy is likely to be maintained for as long as it is feasible,[900] although it is possible in some circumstances that cases could be run on the basis that the *silence* of the corporation on its practices could constitute misleading or deceptive conduct.

[899] This possibility was suggested by an anonymous reviewer of the article that formed the basis of this chapter.

[900] Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (n 493) 1–18.

Consumers may nevertheless find a remedy under other provisions of the ACL, such as those governing unconscionable conduct.

3.3 Unconscionable conduct

3.3.1 Elements of unconscionable conduct

Conduct that is 'unconscionable' is prohibited under sections 21 and 22 of the ACL. The question is: to what extent are the practices involved in digital consumer manipulation liable to be considered as unconscionable? No definition of unconscionability is provided in the sections, and Australian appellate courts have shown a marked reluctance to attempt a precise definition (as discussed in **section 3.3.2** of this chapter).

Section 21 prohibits unconscionable conduct in connection with the actual or possible supply of goods or services. Section 22 sets out a non-exclusive list of matters to which a court may have regard when assessing whether conduct is unconscionable under section 21. Those matters relevant to digital consumer manipulation include:

- relative bargaining power (section 22(1)(a));
- undue influence or pressure, or unfair tactics (section 22(1)(d));
- comparative price (section 22(1)(e));
- consistency of supplier's conduct towards others (section 22(1)(f));
- unreasonable failure to disclose conduct affecting consumer interests or unforeseeable risks to the customer (sections 22(1)(i) and (ii)); and
- the extent to which both parties acted in good faith (section 22(1)(k)).

Additionally, section 21(4)(a)–(c) states as 'interpretative principles' that the doctrine:

a) is not limited by the 'unwritten law' (that is, case law) of unconscionable conduct;

b) applies to 'a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour'; and

c) includes terms and performance, not just formation.

Mirror provisions exist in sections 12CB and 12CC of the ASIC Act regarding the supply of financial services,[901] and are relevant for the same reasons as the mirror provisions relation to misleading or deceptive conduct (discussed in **section 3.2.1** of this chapter).

Section 20 of the ACL (and its mirror provision, section 12CA of the ASIC Act) also prohibits unconscionable conduct 'within the meaning of the unwritten law'. However, it is unlikely that this provision will directly apply to digital consumer manipulation, due to the operation of section 20(2) of the ACL (and section 12CA(2) of the ASIC Act), which excludes conduct prohibited by section 21.

Remedies for breach of the unconscionable conduct provisions are significant. They are similar to those discussed in **section 3.2.1** of this chapter for a breach of section 29 of the ACL, and include pecuniary penalties. However, breach of the unconscionable conduct provisions does *not* attract a criminal remedy.

3.3.2 Meaning of unconscionable conduct

It is difficult to extract from the statute and the cases the precise meaning of 'unconscionable conduct' under section 21. One definition adopted in several decisions is 'showing no regard for conscience; irreconcilable with what is right or reasonable'.[902] However, there remains no judicially accepted 'standard of wrongdoing'.[903] The courts have, deliberately it seems, embraced the ambiguity of sections 21–22 in a sacrifice to flexibility and broadness of

[901] The NSW Court of Appeal in *Tonto Home Loans Australia Pty Ltd v Tavares* [2011] NSWCA 389 (*Tonto v Tavares*) [290] rejected an argument that unconscionability under the ASIC Act had any 'distinct or different meaning' from the equivalent ACL provisions. Remedies may differ: see Gail Pearson, 'The Ambit of Unconscionable Conduct in Relation to Financial Services' (2005) 23 Company and Securities Law Journal 105, 107–09.

[902] *Qantas Airways Ltd v Cameron* (1996) 66 FCR 246, 262; *Hurley v McDonald's Australia Ltd* [1999] FCA 1728 [21]; *Tonto v Tavares* (n 901) [291].

[903] Jeannie Paterson and Gerard Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) 38 Journal of Consumer Policy 331, 343.

applicability, as illustrated in the Full Federal Court decision in *Paciocco v ANZ* where Allsop CJ said:

> In any given case, the conclusion as to what is, or is not, against conscience may be contestable. That is inevitable given that the standard is based on a broad expression of values and norms. [A]ny agonised search for definition, for distilled epitomes or for shorthands of broad social norms and general principles will lead to disappointment, to a sense of futility, and to the likelihood of error. The evaluation is not a process of deductive reasoning predicated upon the presence or absence of fixed elements or fixed rules. It is an evaluation of business behaviour … as to whether it warrants the characterisation of unconscionable, in the light of the values and norms recognised by the statute.[904]

This case was appealed to the High Court, but no criticism was made of Allsop CJ's remarks. Unfortunately, the cases have failed to articulate a clear statement of the 'values and norms recognised by the statute'. A continuing controversy[905] over whether unconscionability requires a 'high level of moral obloquy',[906] 'moral taint',[907] or some other standard[908] has been unhelpful in clarifying the meaning of the section. In particular, the term 'moral obloquy' has been judicially condemned as 'notoriously imprecise'.[909] Even attempted substitutes, such as 'accepted and acceptable community values',[910] have

[904] *Paciocco v Australia & New Zealand Banking Group Ltd* [2015] FCAFC 50 (*Paciocco v ANZ*) [304]. The judge had made a similar point (Bathurst CJ and Campbell JA agreeing) in *Tonto v Tavares* (n 901) [291].

[905] Corones, *The Australian Consumer Law* (n 862) 172–75.

[906] For example, *Paciocco v Australia & New Zealand Banking Group Ltd* [2016] HCA 28 [188].

[907] *Australian Competition and Consumer Commission v ACN 117 372 915 Pty Ltd (in liq) (formerly Advanced Medical Institute Pty Ltd)* [2015] FCA 368 (*ACCC v AMI*) [35]–[36].

[908] Brody and Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (n 898) 171; Paterson and Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (n 903) 342–43.

[909] *Ipstar Australia Pty Ltd v APS Satellite Pty Ltd* [2018] NSWCA 15, [278].

[910] *Australian Competition and Consumer Commission v Lux Distributors Pty Ltd* [2013] FCAFC 90 (*ACCC v Lux*) [23].

provided little assistance to those attempting to assess their own conduct or the conduct of suppliers.

In contrast, the definition of section 20 or 'unwritten law' unconscionability is somewhat clearer due to the seminal High Court decision in *Commercial Bank of Australia Ltd v Amadio*.[911] Here, the court required an 'unfair or unconscientious advantage' to have been taken of a party who was at a 'special disadvantage'.[912] The existence of an *Amadio* 'special disadvantage' may be relevant to the assessment of unconscionable conduct under sections 21–22, but it is not *required*.[913] It also sets a higher standard than is required for sections 21–22 unconscionability. It is generally accepted that Parliament's intention in sections 21–22 was to prohibit a *wider* range of unconscionable conduct than encompassed by the *Amadio* definition, and that this objective has been achieved.[914]

Other than the fact that unconscionability in sections 21–22 is *broader* than in section 20, little more can be said with certainty about the applicable general principles. In 2016, Allsop CJ was optimistic that certainty would develop:

> Over time … the courts will develop principles and legally relevant considerations that will give comfortable form to fact situations … the courts will work through the notion of a business conscience. This is not something foreign to the judicial process.[915]

However, despite the fact that sections 21-22 are on their face technologically neutral, the discussion in **sections 3.3.3** and **3.3.4** of this chapter indicates

[911] *Amadio* (n 836).

[912] Ibid (n 836) [5].

[913] Explanatory Memorandum, Competition and Consumer Legislation Amendment Bill 2010 (Cth) [2.23].

[914] Paul Vout, 'Unconscionability and Good Faith in Business Transactions' (National and Commercial Law Seminar Series, Federal Court of Australia, Monash University Faculty of Law, Commercial Bar Association of Victoria) [9]; Bruce, *Consumer Protection Law in Australia* (n 848) 160; *Australian Competition and Consumer Commission v Simply No-Knead (Franchising) Pty Ltd* [2000] FCA 1365 (*ACCC v Simply No-Knead*).

[915] *Commonwealth Bank of Australia v Kojic* [2016] FCAFC 186 (*CBA v Kojic*) [58].

that, as yet, there is no apparent 'comfortable form' to apply to a fact situation involving digital consumer manipulation.

3.3.3 Choice of flexibility over clarity

The judicial choice of retaining flexibility over 'fixed elements or fixed rules'[916] has been not been challenged in any substantive way by successive governments. The flexibility of sections 21-22 do, on their face, leave room for them to accommodate emerging technologies and data-driven challenges to consumer protection. However, its meaning and effectiveness remain contentious. The relevant doctrine has been criticised by scholars as 'amorphous and ambiguous',[917] 'a category of meaningless reference',[918] and 'generically unhelpful'.[919] Repeated criticism by consumers, small business and downstream suppliers has focussed on the uncertainty of the section, particularly relating to: the lack of specificity in the definition;[920] of the provisions to provide any real guidance to assess whether particular forms of conduct would be considered unconscionable; and difficulties of proof.[921] Attempts by businesses and consumers to apply the unconscionability provisions in any meaningful way to emerging technologies will face significant challenges.

---

[916] *Paciocco v ANZ* (n 904) [304].

[917] *Attorney-General (NSW) v World Best Holdings* [2005] NSWCA 261 [118].

[918] Charles Rickett, 'Unconscionability and Commercial Law' (2005) 24 University of Queensland Law Journal 73, 73.

[919] Lynden Griggs and Eileen Webb, 'Section 22 Unconscionability: A Sauropod in Need of Life Support' (2011) 11 Law and Justice Journal 31, 32.

[920] Similar arguments have been made in relation to the prohibition of unconscionability in the US Uniform Commercial Code 2-302 and its antecedents. See Robert E Scott and Jody S Kraus, *Contract Law and Theory* (5th edn, LexisNexis 2013) 501; Arthur Allen Leff, 'Unconscionability and the Code: The Emperor's New Clause' (1967) 115 University of Pennsylvania Law Review 485.

[921] Submissions to the Australian Government's Competition Policy Review held over 2014–15 (also known as the 'Harper Review'), in particular submissions of AgForce Queensland, 2; Australian Chicken Growers' Council Limited, 7-8; Australian Dairy Farmers Limited, 9-10; Australian Newsagents' Federation, 11; and National Farmers' Federation, 7. See Australia, 'Issues Paper Submissions' (*Competition Policy Review*, 2014) <http://competitionpolicyreview.gov.au/issues-paper/submissions/> accessed 1 November 2017.

Additionally, several other problems with statutory unconscionable conduct have been identified, relevantly:

- the lack of familiarity with, and understanding of, the term 'unconscionability' outside of the courts, particularly by business and consumers;[922]
- a high threshold level of misconduct,[923] in that conduct which is merely unfair,[924] or where one party has more bargaining power than the other,[925] is unlikely to be considered as unconscionable without additional factors;
- uncertainty as to the applicability of the factors in section 22 (discussed further below in this section); and
- practical enforcement difficulties due to vulnerable victims either being unable to bring actions themselves or providing poor testimony for regulator actions.[926]

[922] Sarida McLeod, 'Statutory Unconscionable Conduct under the ACL: The Case Against a Requirement for "Moral Obloquy"' (2015) 23 Competition and Consumer Law Journal 123, 129; Paterson and Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (n 903) 352; Brody and Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (n 898) 169.

[923] Brody and Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (n 898) 170. See in particular the formulation in *Australian Competition and Consumer Commission v Allphones Retail Pty Ltd (No 2)* [2009] FCA 17 (*ACCC v Allphones*) [113] which requires that 'the actions of the alleged contravenor show no regard for conscience, and be irreconcilable with what is right or reasonable' (although note that this was an interlocutory application).

[924] *ACCC v AMI* (n 907) [39].

[925] *CG Berbatis Holdings Pty Ltd v Australian Competition and Consumer Commission* [2001] FCA 757 (*Berbatis*); Australian Securities and Investments Commission, *Submission No 1 Supplementary to Submission No 45 to Senate Standing Committee on Economics, The Performance of the Australian Securities and Investments Commission* <www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/ASIC/Submissions> 6.

[926] Brody and Temple, 'Unfair But Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (n 898) 171.

The contention surrounding the doctrine has led to multiple government and parliamentary inquiries since the introduction of statutory unconscionability in 1986.[927] There have been repeated requests to legislate for a specific definition, or to include a list of examples of unconscionable conduct in the ACL (as was done for the unfair contract terms provisions).[928] The government and parliamentary inquiries have led to some restructuring of the sections and amendments to supporting wording, such as the introduction of section 21(4). But on the whole, successive governments have refused requests for more specificity. Instead, it has been recommended that the ACCC run test cases[929] and issue guidance.[930] However, the ACCC's current guidance document for business does not inspire confidence: it begins its explanation of the term with the words '[u]nconscionable conduct can be a difficult concept to understand'.[931]

---

[927] Michelle Sharpe and Christine Parker, 'A Bang or a Whimper? The Impact of ACCC Unconscionable Conduct Enforcement' (2007) 15 Trade Practices Law Journal 139, 142 provides a list of *eleven* 'government reports recommending for or against unconscionable conduct provisions'. There have also been many others since 2007, for example: Australia, Senate Standing Committee on Economics, 'The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974' (December 2008); Australia, Treasury, 'The Nature and Application of Unconscionable Conduct Regulation: Can Statutory Unconscionable Conduct be Further Clarified in Practice?' (Issues Paper, November 2009); Australia, 'Commonwealth Government Response to the Senate Standing Committee on Economics Report on "The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974"' (November 2009); Bryan Horrigan, David Lieberman and Ray Steinwall, *Strengthening Statutory Unconscionable Conduct and the Franchising Code of Conduct* (Expert Panel Report to the Treasury and the Department of Innovation, Science and Research, February 2010); Ian Harper and others, *Competition Policy Review: Final Report (Harper Review)* (March 2015); Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review: Final Report* (n 76).

[928] ACL s 25.

[929] Australia, 'Commonwealth Government Response to the Senate Standing Committee on Economics Report on "The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974"'(n 927).

[930] Horrigan, Lieberman and Steinwall, *Strengthening Statutory Unconscionable Conduct and the Franchising Code of Conduct* (n 927).

[931] Australian Competition and Consumer Commission, *Business Snapshot: Unconscionable Conduct* (12 September 2012) <www.accc.gov.au/publications/business-snapshot/unconscionable-conduct> accessed 30 June 2018.

Section 22, which contains a non-exclusive list of matters that *can* be considered in an assessment of unconscionability, could have provided more fertile ground to ensure that the doctrine was given real content. However, the section itself gives no guidance on the extent to which these factors or others should be considered, and judicial guidance has been inconsistent. Some decisions discuss the factors explicitly.[932] Others do not mention them at all,[933] although arguably they are nevertheless identifiable in *some* cases without specific reference.[934] No formula has been adopted for ascertaining how many, or to what extent, factors must be present.[935] It is worth noting, however, that the cases indicate that it is not necessary to show that one factor is determinative. A number of factors can be aggregated and a decision made based on 'all the circumstances'.[936] As to the importance of individual factors, it appears that inequality of bargaining power, without more, is insufficient,[937] and similarly, inadequate disclosure.[938] However, little more than that of *general* principle can be drawn from the cases.

Many cases of digital consumer manipulation could be considered as cases of 'undue influence or pressure', or 'unfair tactics', which are factors under section 22(1)(d) to which the court may have regard in making a decision about unconscionable conduct. There are several cases where inappropriate pressure or unfair tactics have been considered unconscionable.[939] However, these generally involve face-to-face or telephone contact between the seller

[932] *Australian Competition and Consumer Commission v Keshow* [2005] FCA 558; *ACCC v Simply No-Knead* (n 914); *ACCC v AMI* (n 907); *NRM Corp Pty Ltd v Australian Competition and Consumer Commission* [2016] FCAFC 98 (*NRM v ACCC*).

[933] For example, *Tonto v Tavares* (n 901); *ACCC v Lux* (n 910).

[934] For example, *National Exchange v ASIC* (n 882).

[935] Bruce, *Consumer Protection Law in Australia* (n 848) [6.10].

[936] *NRM v ACCC* (n 932) [183]; *ACCC v Allphones* (n 923) [114]; *Dukemaster* (n 841) [17].

[937] *Berbatis* (n 925); *Australian Competition and Consumer Commission v Samton Holdings Pty Ltd* [2002] FCAFC 4.

[938] *Australian Competition and Consumer Commission v Oceana Commercial Pty Ltd* [2004] FCAFC 174.

[939] *ACCC v Lux* (n 910); *ACCC v AMI* (n 907); *Australian Competition and Consumer Commission v Origin Energy Electricity Ltd* [2015] FCA 55.

representatives and the consumers.[940] Commonly (although not exclusively),[941] some aspect of the conduct breached, or was likely to breach, other sections of the ACL, such as the door-to-door selling provisions,[942] unsolicited consumer agreement provisions,[943] and/or the prohibitions on misleading or deceptive conduct, and false and misleading representations.[944] In *ACCC v AMI* (discussed further at **section 3.3.4** of this chapter) considerable emphasis was placed on the nature of the misconduct emanating from a medical practice, 'which characteristically make[s] patient welfare a primary concern'.[945] On its face, sections 21–22 unconscionability does *not* require a breach of other laws, an *Amadio*-style 'special disadvantage', or a duty above and beyond that of a normal business to its customers; but it remains uncertain where the line can be drawn. It also remains to be seen whether judges will be convinced that marketing messages delivered by SMS, a digital personal assistant such as Max (**Vignette J3**), a doll such as Ella (**Vignette J11**) or other non-human means have the same persuasive force as 'real person' (face-to-face or over the phone) high-pressure selling. Further public empirical research on the

[940] For example, *Australian Securities and Investments Commission v Malouf Group Enterprises Pty Ltd* [2018] FCA 808 (*ASIC v Malouf*); *Ibrahim v SCE Solar City Enterprises Pty Ltd* [2017] NSWCATCD 96 (*Ibrahim v SCE*); *Australian Competition and Consumer Commission v Get Qualified Australia Pty Ltd (in liq) (No 2)* [2017] FCA 709 (*ACCC v Get Qualified*); *Australian Competition and Consumer Commission v Acquire Learning & Careers Pty Ltd* [2017] FCA 602; *Australian Competition and Consumer Commission v Clinica Internationale Pty Ltd (No 2)* [2016] FCA 62 (*ACCC v Clinica*); *ACCC v Lux* (n 910); *ACCC v Origin* (n 939); *Australian Competition and Consumer Commission v Titan Marketing Pty Ltd* [2014] FCA 913.

[941] See for example, *National Exchange v ASIC* (n 882).

[942] For example, *ACCC v Get Qualified* (n 940); *ACCC v Acquire* (n 940); *ACCC v Origin* (n 939); *ACCC v Titan* (n 940); *ACCC v Lux* (n 910).

[943] For example, *Australian Competition and Consumer Commission v Nuera Health Pty Ltd (in liq)* [2007] FCA 695; *ACCC v Titan* (n 940); *ACCC v Origin* (n 939); *ACCC v Clinica* (n 940); *ACCC v Acquire* (n 940); *ACCC v Get Qualified* (n 940); *Ibrahim v SCE* (n 940); *ASIC v Malouf* (n 940).

[944] *ACCC v Lux* (n 910).

[945] *ACCC v AMI* (n 907) [905]. Some form of expected commitment to patient welfare was mentioned by the trial judge seven times throughout the judgment.

effectiveness of this would assist, as currently most such experimentation is proprietary to the marketing companies profiting from it.[946]

3.3.4 Digital consumer manipulation as predatory business conduct

Despite the problems discussed in **section 3.3.3** of this chapter, some assistance can be found in two places. First, in 2015, Paterson and Brody conducted a detailed analysis of the judicial treatment of 'predatory business conduct'.[947] They examined cases involving 'business models whose very operating premise relies upon taking advantage of the reduced ability of the consumers … to protect their own interests'.[948] They concluded that Australian courts have generally been successful in applying the unconscionable conduct provisions in the ACL and the ASIC Act to respond appropriately to a broad selection of predatory business conduct,[949] such as funeral insurance, payday lending, and sale of inappropriate educational services to those dependent on social security payments.[950]

Second, the distaste of judges for predatory business conduct, especially that targeting vulnerability, is reflected in two important recent Full Federal Court decisions, *National Exchange v ASIC*[951] and *ACCC v AMI*.[952] In the former case, the Full Federal Court held National Exchange had breached the relevant unconscionable conduct provisions of the ASIC Act.[953] The subject of the case was National Exchange's offer to shareholders of Aevum to

[946] Nadler and McGuigan, 'An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing' (n 647).

[947] Paterson and Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (n 903).

[948] Ibid (n 903) 332.

[949] Ibid 346.

[950] Ibid 332.

[951] *National Exchange v ASIC* (n 882).

[952] *ACCC v AMI* (n 907).

[953] In this case, the relevant section breached was s 12CC, a mirror provision to s 51AC of the then Trade Practices Act 1974 (Cth). The corresponding new provisions are ACL ss 21–22, and ASIC Act ss 12CB and 12CC.

purchase their shares at a price well under market value. An accurate estimate of the shares' market value was included on the reverse side of the offer document. The company's controller admitted targeting members of demutualised companies that he believed were more likely to accept less than fair value.

The Full Federal Court held that the offer document was not *misleading* or *deceptive*.[954] However, the targeting of inexperienced members and the framing of the document was held to be *unconscionable* because:

> National Exchange set out to systematically implement a strategy to take advantage of … a group of inexperienced persons who would act irrationally from a purely commercial viewpoint and would accept the offer. They were perceived to be vulnerable targets and ripe for exploitation, as they would be likely to act inadvertently and sell their shares without obtaining proper advice, and they were a predictable class of members from whom [National Exchange] could procure a substantial financial advantage by reason of their commercially irrational conduct … This is not a case of obtaining a low price by shrewd negotiation. It is predatory conduct designed to take advantage of inexperienced offerees …[955]

ACCC v AMI[956] concerned a claim of unconscionable conduct under the ACL relating to the marketing activities of a medical clinic. The trial judge, North J, (with whom the Full Federal Court agreed)[957] discussed in detail the impact of AMI's high-pressure selling techniques in 'targeting vulnerability', specifically the vulnerability of those seeking treatment for perceived sexual dysfunction. The judge, in finding AMI's conduct in breach of section 21, declared that AMI's 'technique of selling was prone to rob men of independent judgement'.[958] He also adjudged it 'immoral to seek to harness

[954] *National Exchange v ASIC* (n 882).
[955] Ibid [43].
[956] *ACCC v AMI* (n 907).
[957] The appeal was heard as *NRM v ACCC* (n 932).
[958] *ACCC v AMI* (n 907) [896].

the fears and anxieties of men suffering from [erectile dysfunction] or [premature ejaculation] for the purpose of selling medical treatments'.[959]

One view is that some forms of digital consumer manipulation could be even more severe, or against conscience, than the predatory business models discussed above. Digital consumer manipulation in some cases is not marked by mere opportunism, but by a deliberate *intent* to track down, or even create, circumstances in which a vulnerability is likely to operate most strongly, and then to take advantage of it.[960] Therefore, it appears possible that at least some digital consumer manipulation techniques would fall foul of the unconscionable conduct prohibitions. In **Vignette J11**, marketing disguised as a conversation between nine-year-old Mylin and Ella, a doll to which she is emotionally attached, may indeed be considered unconscionable. If a marketer has access to and implements in its algorithms behavioural research that shows fatigue, blood sugar levels and time of day significantly affecting willpower, then unhealthy 'nudges'[961] to Fahim, who has been identified as a diabetic, may also be seen as sufficiently predatory to contravene the provisions.

This result is supported by the words of the statute, particularly section 21(4)(b). This sub-section indicates that section 21 'is capable of applying to a system of conduct or pattern of behaviour, whether or not a particular individual is identified as having been disadvantaged by the conduct or behaviour'. The wording of this sub-section suggests there is no need for proof that *actual* consumer disadvantage has resulted from the scrutinised conduct. Another possible consequence of section 21(4)(b) is that an *attempt* to exploit consumers (even if unsuccessful) may be sufficient to breach the section. This is particularly noteworthy as the actual effectiveness of some behavioural marketing techniques is still controversial, as discussed

[959] Ibid.

[960] Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 38) 160.

[961] Richard H Thaler and Cass R Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale UP 2008).

in **section 3.3.1** of **Chapter 5**.[962] The lack of a requirement to prove the behaviour's effectiveness or actual consumer disadvantage could stifle potential defences by suppliers, making it easier for regulators to bring an action.

One possible counterpoint to this view is contained in two cases involving problem gamblers, both brought against the owners of the Crown Casino, Crown Melbourne Ltd (**Crown**). These cases show a judicial predisposition to assuming that consumers are perfectly rational and must look after themselves, even when their psychological traits, such as a gambling addiction or disorder, make doing so difficult. In the High Court decision of *Kakavas v Crown,*[963] Mr Kakavas suffered from a gambling addiction, which was known to Crown (at least constructively). However, this was dismissed as a basis for a holding of unconscionable conduct under section 20 and the 'unwritten law' on unconscionable conduct. The court held that Mr Kakavas, who was a wealthy 'high-roller' gambler, did not suffer an *Amadio*-style 'special disadvantage', as the court considered his gambling problem did not make him incapable of making rational decisions (including self-exclusion).[964] The court did concede that the result may have been different where a gambler was obviously drunk, young, old or 'incompetent'.[965]

A few years after the *Kakavas v Crown* decision, a group of individuals who had suffered large losses on poker machines brought a case against Crown and the supplier of the poker machines (Aristocrat Technologies Australia Pty Ltd). In *Guy v Crown,*[966] the plaintiffs alleged that the design of the Dolphin Treasure electronic gaming machine constituted unconscionable conduct in relation to players who were 'vulnerable to becoming habituated and/or addicted to playing'[967] this particular kind of poker machine. In

[962] See n 678 and n 679.
[963] *Kakavas v Crown Melbourne Ltd* [2013] HCA 25 (*Kakavas v Crown*).
[964] Ibid.
[965] Ibid [30].
[966] *Guy v Crown* (n 880).
[967] Ibid (n 880) [465].

finding against the plaintiffs in this case, Mortimer J emphasised that it was a 'significant challenge' to prove that those with a gambling problem or disorder had '*no* capacity to make judgments for themselves'.[968] On a strict construction of the court's language, both *Kakavas v Crown* and *Guy v Crown* would set a very high bar for proof in their 'all or nothing' attitude. A gambler must be rendered totally incapable of making rational decisions in order for unconscionability to be found. It would appear that *impaired* capacity, even significantly impaired capacity, is insufficient. As with gambling, a proof of *total* incapacity in relation to digital consumer manipulation is surely an unattainable goal.

However, the application of these two cases to conduct in a wider context is uncertain, for a number of reasons. In *Kakavas v Crown* the High Court emphasised the uniqueness of the activity involved: 'gambling transactions are a rare, if not unique species of economic activity in a civilised community, in that each party sets out openly to inflict harm on the counterparty'.[969] In contrast, consumers subject to digital consumer manipulation techniques are rarely setting out to inflict harm on anyone, and may well be unaware that they are engaging in any activity other than their normal day-to-day lives, unlike when they visit a casino or an online gambling site. Additionally, *Kakavas v Crown* was decided solely on the basis of a predecessor provision to section 20. However, Mortimer J's decision in *Guy v Crown* suggests that there may be some applicability to the broader notion embodied in sections 21–22. Mortimer J's 'no capacity' comments in *Guy v Crown* related specifically to the section 20 case and the assessment of a special disadvantage. However, in dismissing an additional claim based on unconscionable conduct in sections 21–22, Mortimer J stated that her reasoning on this point in relation to the section 20 case had 'some application'[970] to her decision on the sections 21–22 case. However, Mortimer J also acknowledged that '[t]here are real debates to be had, on the law and

[968] Ibid (n 880) [495] (emphasis added).
[969] *Kakavas v Crown* (n 963) [25].
[970] *Guy v Crown* (n 880) [476].

on the facts … in relation to the state of research and knowledge about gambling addictions, and pathways to addiction'.[971]

3.3.5 Conclusion

Consumers, regulators and advocacy organisations may find more useful protections for the more egregious forms of digital consumer manipulation under the statutory doctrine of unconscionable conduct than under a misleading or deceptive conduct claim. While the scope of the statutory doctrine is still undefined, the breadth of the potential definition of unconscionable conduct makes it likely that many forms of digital consumer manipulation will fall foul of the prohibition.

However, the operation of the unconscionability provisions in the face of digital consumer manipulation is *uncertain*, one of the categories of legal problems set out in **section 2.2.1.2** of **Chapter 3**. The lack of a useful definition of unconscionability, in addition to the lack of analogous cases, makes it difficult to assess when and where digital consumer manipulation techniques would constitute unconscionable conduct. The uncertainty about what is considered 'unconscionable' is exacerbated by the current lack of clear societal norms about the acceptability of digital consumer manipulation, and the inability of the courts and Parliament to articulate real and useful content for the concept.

Judicial and parliamentary attitudes have certainly made the unconscionable conduct provisions flexible, but at a cost. The concept of unconscionable conduct is 'technologically neutral', so there is nothing on its face preventing the section from applying appropriately to digital consumer manipulation and other forms of sociotechnical change. However, the failure of courts to articulate details of a test or principles to give content to the term 'unconscionable' make it difficult for business and consumers to assess whether particular forms of new conduct, such as digital consumer manipulation, are indeed unconscionable. This uncertainty also provides a deterrent to bringing cases, particularly by consumers, but also by regulators.

[971] Ibid [460].

Governments may encourage the running of test cases, but they do not generally provide unlimited (or even particularly adequate) budgets to do so.

3.4 Unsolicited consumer agreements

In *ACCC v Lux*, the Full Federal Court observed that the objective of the ACL provisions on unsolicited consumer agreements[972] 'was to promote the operation of fair and efficient markets, by providing appropriate consumer protection when the consumer is subject to vulnerability or disadvantage due to the nature of the sales process'.[973] However, in their current form, these provisions poorly target digital consumer manipulation techniques, as they apply only in circumstances where the sellers use digital data collection techniques combined with non-digital marketing channels. Nonetheless, it is useful to examine these provisions because they recognise a form of consumer vulnerability existing without a need to prove an error by the consumer or some form of conduct 'against conscience' by the seller.

Unlike the ACL provisions relating to misleading or deceptive conduct or false or misleading representations, the unsolicited consumer agreements provisions do not require falsehood or error. Rather, the drafters assumed that certain types of sales automatically subjected consumers to 'added vulnerability or disadvantage',[974] therefore requiring heightened protections. These sales are limited to unsolicited telephone sales and physical 'in-person' sales outside of the supplier's place of business (section 69(1)(b)). In these types of sales, the additional consumer protections include restricted hours (section 73), pre-contractual disclosures (section 74); a mandatory cooling-off period (sections 76, 79, 82–85, 87, 88) and time restrictions on payment and delivery (section 86).

Some forms of digital consumer manipulation may be regulated by these provisions. Suppliers may use new data gathering and data analytic

[972] ACL pt 3-2, div 2.

[973] *ACCC v Lux* (n 910) [10].

[974] Second Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth), Regulatory Impact Statement [23.52].

capabilities and behavioural research to plan face-to-face or telephone approaches. In this case, the reach and impact of those approaches will be limited by the provisions. However, where digital consumer manipulation techniques involve digital rather than 'in person' or telephone approaches, they will not usually be regulated under the provisions, due to the operation of section 69. For example, in **Vignette J9**, if Max's updating of Jessica's profile to indicate she was feeling insecure about her appearance triggered a callout to a Couteux salesperson to visit her house, then the section would be triggered (assuming the price threshold limits were reached).[975]

Negotiations must be 'in each other's presence'[976] in order to trigger the protection offered by the relevant provisions, precluding purely digital approaches. Exclusion of digital approaches may have been appropriate when such approaches were limited to generic texts or emails. However, suppliers may have the ability to know when an individual consumer is likely to be most vulnerable to making a particular purchasing decision. Additionally, they may have the capacity to offer goods or services via a method that is easy to anthropomorphise, such as a doll (like Ella), robot pet, or digital personal assistant (like Max) speaking to them with a human voice and offering empathy and companionship. In such cases, it may be difficult to justify that this is less exploitative than an approach by a real person.

If unconscionability is too broad and 'technologically neutral' to be a useful means of regulation, these provisions exemplify the opposite. 'Where similar harms and risks can arise as a result of diverse things or practices, then designing a rule or regime around only some of those things or practices is poorly targeted.'[977] In the face of digital consumer manipulation, this regulation is poorly targeted because it is too specific. It concentrates on the technical means by which an end is achieved, and leaves behaviours resulting in similar outcomes unchecked: that is, the creation of a vulnerability eroding consumer autonomy and choice. However, with enabling

[975] ACL s 69(d).

[976] ACL s 69(1)(b)(i).

[977] Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 586.

amendments these provisions could provide a model for regulating *some* types of digital consumer manipulation, such as entering into contracts mediated through digital personal assistants or healthcare robots. However, it would be more difficult to implement a similar scheme when the influence is digital but the transaction is concluded elsewhere, such as in the case of Jessica's purchase of beauty products in **Vignette J12**.

3.5 Other areas of relevant law

Other areas of relevant law worthy of further research are outside the scope of this dissertation; they include unfair contract terms,[978] regulation of financial advice,[979] and advertising of therapeutic goods.[980] Most are unlikely to apply to digital consumer manipulation generally, but rather to specific instances. The unfair contract terms regime is more general, but since it excludes terms relating to subject matter and price,[981] which are usually the most prominent in deciding whether to enter into a consumer contract, this section of the ACL has been excluded from the scope of this dissertation.

Other legal and equitable doctrines directed against questionable practices in commercial dealings may also be worthy of further research, such as undue influence, undue harassment, duress and mistake. These are discussed briefly in **section 3.5.4** of this chapter. However, they are unlikely to provide substantial *additional* protection for a consumer who has been subject to digital consumer manipulation, as they tend to apply in far narrower circumstances than does the doctrine of statutory unconscionable conduct.

The omission of a detailed analysis of data protection legislation from this dissertation requires more substantial justification. While the regulation of marketing practices has traditionally been the domain of the ACL and its

[978] ACL pt 2-3.

[979] See for example, Corporations Act 2001 (Cth) pts 7.7–7.7A; Australian Securities and Investments Commission, *Regulatory Guide 121: Doing Financial Services Business in Australia* (July 2013).

[980] For example, Therapeutic Goods Act 1989 (Cth) s 42BAA mandates compliance with the Therapeutic Goods Advertising Code (No 2) 2018 (Cth). This Code came into effect on 1 January 2019.

[981] ACL s 26.

predecessors, misuse of consumer data is usually seen as falling under the remit of the Privacy Act, and, to a much more limited extent, the Spam Act.

3.5.1 Privacy Act

However, this section outlines some serious barriers to relying upon the Privacy Act to protect consumers from data-related harms.

First, there are many gaps in the Privacy Act's protections. Threshold requirements exclude many businesses from its operation.[982] There are also other important exemptions from some of its provisions, such as disclosures to related bodies corporate,[983] acts or practices outside Australia[984] and employee records.[985]

Second, many types of consumer data may not be subject to the Privacy Act, as demonstrated in the recent decision in *Privacy Commissioner v Telstra*,[986] where journalist Ben Grubb sought access to metadata held by Telstra relating to his use of telecommunications services. Both the Administrative Appeals Tribunal (**AAT**)[987] and the Full Federal Court[988] on appeal proposed a narrow construction of the meaning of personal information 'about an individual'. The Full Federal Court considered that the colour of Grubb's mobile phone and his network type was not information *about* Grubb, and therefore not personal information.[989] Similarly, the AAT gave an example of car service records, and stated that these would not constitute information 'about' the car's owner, even if the records contained the owner's name and

[982] In particular, s 6D of the Privacy Act 1988 (Cth) excludes businesses with AUD3 million or less in annual turnover, unless they hold health information, are a credit reporting body or a Commonwealth contractor, or deal in personal information.

[983] Privacy Act 1988 (Cth) s 13B.

[984] Ibid s 6A.

[985] Ibid s 7B.

[986] *Privacy Commissioner v Telstra Corp Ltd* [2017] FCAFC 4.

[987] *Telstra Corp Ltd and Privacy Commissioner* [2015] AATA 991.

[988] *Privacy Commissioner v Telstra* (n 986).

[989] Ibid (n 986) [64].

the car's registration number.[990] Significant uncertainty still remains as to its meaning,[991] including in the case of eObjects.[992] The definition of 'personal information' in the Privacy Act has since been reworded, but the rewording did not clarify the scope of information being 'about an individual'. If similar reasoning to the Full Federal Court and the AAT in the *Telstra* case is adopted in subsequent cases, much information of value to consumers and third parties is likely to fall outside this definition.

Third, enforcement mechanisms are weak, particularly for consumers. No direct right of action is available to consumers, although under section 36 of the Privacy Act they may make a 'complaint' to the regulator, the OAIC. OAIC decisions relating to complaints are only subject to appeal where the OAIC makes a 'determination' under section 52 of the Privacy Act. Few such determinations have been made under this provision,[993] and this has resulted in a paucity of appellate jurisprudential development. Also, *competitors* have no right of action under the Privacy Act. Under section 18 of the ACL and its predecessors, competitor actions have provided significant impetus to enforcement of the misleading or deceptive conduct provisions.[994]

Additionally, the sanctions that have been applied have been insubstantial (for example, enforceable undertakings). Where compensation has been

[990] *Telstra Corp and Privacy Commissioner* (n 987) [96]. See also Joshua Yuvaraj, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (2018) 34 Computer Law and Security Review 47, 53.

[991] Yuvaraj, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (n 990) 53–54.

[992] Peter Leonard, 'A Review of Australian Privacy Commissioner v Telstra Corporation Limited' (*Gilbert + Tobin Lawyers*, 16 February 2017) <www.gtlaw.com.au/insights/review-australian-privacy-commissioner-v-telstra-corporation-limited> accessed 16 January 2019, 4.

[993] See Graham Greenleaf, 'Privacy Enforcement in Australia Is Strengthened: Gaps Remain' (2014) 128 Privacy Laws & Business International Report 1. The relevant page reference (4) is from the SSRN version <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2468774> accessed 16 January 2019.

[994] See for example, *Hornsby Building Information Centre Pty Ltd v Sydney Building Information Centre Ltd* [1978] HCA 11; *Parkdale v Puxu* (n 850); *Campomar* (n 877); *Telstra Corp Ltd v Singtel Optus Pty Ltd* [2014] VSC 35.

awarded,[995] the amounts have been too small to have any meaningful deterrent effect. No civil penalties (available up to AUD2.1 million) have been awarded since their introduction in 2014, standing in stark contrast to some other jurisdictions such as the UK.[996] Insufficient funding and resourcing of the OAIC, restricting its capacity to bring actions, has also been the subject of public criticism.[997]

Further, and most importantly, 'consent' overrides most safeguards for consumers in relation to the use of consumer data, and its transfer to third parties. The consent required is weak, and its adequacy to protect data subjects has been vigorously contested.[998] Commercial entities are permitted to deal with consumer data even though in most cases the nominal consumer consent obtained is not informed, is non-negotiable, and is subject to unilateral interpretation and extension at the will of the commercial party. In some cases, such as in direct marketing, where it is 'impracticable to obtain consent',[999] even the requirement of weak consent is disregarded. This problem is exacerbated by forms of consent and privacy policies that are lengthy, difficult to understand, ambiguous, hard to find, vague and/or overly broad.[1000] Empirical evidence suggests this encourages consumers not

[995] Office of the Australian Information Commissioner, 'Determinations' <www.oaic.gov.au/privacy-law/determinations/> accessed 24 April 2018.

[996] Information Commissioner's Office, 'Actions We've Taken' <https://ico.org.uk/action-weve-taken/enforcement/> accessed 24 April 2018.

[997] For example, Allie Coyne, 'Starved of Funding, Resources, OAIC is Left to Shrivel' (*IT News*, 17 July 2015) <www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273> accessed 23 March 2018; Denham Sadler, 'Privacy Office at Breaking Point' (*InnovationAus,* 26 March 2018) <www.innovationaus.com/2018/03/Privacy-office-at-breaking-point> accessed 5 March 2018; Ben Grubb, 'Australia's Privacy Watchdog is "Woefully" and "Criminally" Underfunded' (*Crikey*, 16 July 2018) <www.crikey.com.au/2018/07/16/australias-privacy-watchdog-is-woefully-and-criminally-underfunded/?ft=SGxCKzkvcXRVNWkoeU1tcjdPcGlNQT09> accessed 14 February 2019.

[998] Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report 108, May 2008) 674–83.

[999] For example, Privacy Act 1988 (Cth) sch 1, Australian Privacy Principle 7, which regulates direct marketing.

[1000] Joel R Reidenberg and others, 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45 The Journal of Legal Studies S163; Bosua and others, 'Privacy in

to read most policies or to helplessly accept unfavourable terms because '[i]t [is] the only way to access the product or service'.[1001] For all of these reasons, the Privacy Act is limited in its protections against digital consumer manipulation.[1002]

3.5.2 Spam Act

Enforcement of the Spam Act has been modestly more effective than the Privacy Act in restricting the delivery of unwanted marketing messages. However, the provisions of the Spam Act arguably suffer from excessive technological specificity (as discussed in **section 2.2.1.3** of **Chapter 3**), leading to a very narrow application. The legislation is limited to messages sent to electronic addresses in connection with an email, instant messaging, telephone account or similar.[1003] Like the Privacy Act, the Spam Act also contains overriding express or 'inferred' consent exclusions.[1004]

3.5.3 The benefits of a consumer law perspective

Consumer law remains a more fertile area than either current privacy or spam legislation for examining the existence of effective mechanisms. Consumer law may lack a coherent and 'overarching theory of consumer

---

a World of the Internet of Things: A Legal and Regulatory Perspective' (n 102) 10; Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2) 76–80.

[1001] Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) Table 4, 59.

[1002] This analysis of the weaknesses of the Privacy Act 1988 (Cth) was published by the author of this dissertation in the article Manwaring, 'Will emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (n 110) 175–77, which was published online on 3 December 2018. A week later, on 10 December 2018, the ACCC released its preliminary report as part of the Digital Platforms Inquiry, which contained a recommendation that the Privacy Act 1988 (Cth) be amended to: '(a) strengthen notification requirements; (b) introduce an independent third-party certification scheme; (c) strengthen consent requirements; (d) enable the erasure of personal information; (e) increase the penalties for breach; (f) introduce direct right of action for individuals; (g) expand … resources for the OAIC to support further enforcement activities.' Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (n 82) 223.

[1003] Spam Act s 5.

[1004] Ibid s 16(2), sch 2.

protection',[1005] but there is at least one theme to be drawn from the ACL that has significant potential to assist consumers when dealing with eObjects. Specifically, the drafters of the ACL and its predecessors recognised that 'consent' is insufficient to absolve sellers of responsibility for their marketing activities, and that consumers need to be protected against seller misconduct even when they have said 'yes' to a transaction. This normative outlook is demonstrated by the nature of the marketing and selling protections contained in the ACL: for example, the prohibitions against misleading or deceptive conduct and false or misleading representations (sections 18 and 29), unconscionable conduct (sections 20–22), unfair contract terms (sections 23–27), harassment and coercion (section 50), and the cooling-off period required under the unsolicited consumer agreements provisions (sections 69–95). All of these provisions can be characterised as presuming that the conduct regulated detrimentally affects the quality of a consumer's consent to entering into a transaction, or to the terms which are offered. It also assumes that this effect on consent is unacceptable, and should be prohibited or mitigated in some way.

There exists a fundamental acknowledgement in the ACL that 'consent' is not sufficient to protect consumers in a broad range of circumstances. This acknowledgment provides a more sensible, and consumer-friendly, framework than the Privacy Act's enshrining of the paramountcy of consent despite its demonstrated inadequacies. The comparative strength and activity of the ACL regulators (namely the ACCC and state and territory fair trading agencies)[1006] as compared to the OAIC, also displays an advantage for consumer protection law over Australia's current data protection legislation.

[1005] Bruce, *Consumer Protection Law in Australia* (n 848) [1.9]. See also Norbert Reich, 'Diverse Approaches to Consumer Protection Philosophy' (1992) 14 Consumer Issues in Law, Economics and Behavioural Sciences 257, 257; Lynden Griggs, 'Intervention or Empowerment: Choosing the Consumer Law Weapon!' (2007) 15 Competition & Consumer Law Journal 111.

[1006] Access Canberra (Australian Capital Territory) and others, 'Compliance and Enforcement: How Regulators Enforce the Australian Consumer Law' (January 2017) <https://cdn.tspace.gov.au/uploads/sites/86/2019/01/ACL_Compliance_and_enforcement_guide.pdf> accessed 30 June 2017. The state and territory fair trading agencies

3.5.4 Undue harassment, undue influence, duress and mistake

Other legal and equitable doctrines targeted at questionable practices in commercial dealings are unlikely to provide substantial additional protection for a consumer who has been subject to digital consumer manipulation. However, they may be useful in some limited situations, particularly if they are used to support a broader claim of unconscionable conduct.[1007]

3.5.4.1 Undue harassment

Section 50 of the ACL, which prohibits undue harassment or coercion, may apply to a limited range of digital consumer manipulation situations. For example, in **Vignette J11**, imagine that the Internet-connected doll, Ella, was programmed to tell the human child, Mylin, on the hour, every hour, that she must buy a specific brand of doll to be a friend for Ella when she gets lonely. In European jurisdictions, this would constitute a clear breach of laws implementing Article 5 and section 28 of Annex I of the EU's *Unfair Commercial Practices Directive*.[1008] In Australia, this conduct *may* well amount to undue harassment, by analogy with persistent telephone solicitations, conduct that the ACCC considers a breach of section 50.[1009] However, many cases of digital consumer manipulation would rely on more subtle marketing approaches, such as less frequent or less direct approaches, which are less likely to breach section 50.

---

are: Access Canberra (ACT); NSW Fair Trading; Northern Territory Consumer Affairs; Office of Fair Trading (Qld); Consumer and Business Services (SA); Consumer Affairs Victoria; Department of Commerce (WA).

[1007] For example, *ACCC v Lux* (n 910), which contained a finding of unconscionable conduct based partially on breach of door-to-door selling laws; *Australian Competition and Consumer Commission v Lifestyle Photographers Pty Ltd* [2016] FCA 1538, where misleading or deceptive conduct under s 18 of the ACL and false representations under s 29 provided partial foundation for a holding of unconscionable conduct.

[1008] Unfair Commercial Practices Directive (EU) (n 831).

[1009] Australian Competition and Consumer Commission, *Advertising and Selling Guide* (November 2017) 37.

3.5.4.2 Duress or mistake

In 2016, Mik undertook a substantial analysis of digital consumer manipulation in relation to 'conventional' online contracting based on UK law.[1010] As part of this analysis, Mik dismissed the likelihood of substantial intervention of the doctrines of duress and mistake, due to the former's requirement of a 'wrongful or illegitimate threat',[1011] and the latter's constraint that '[t]he mistake must pertain to the terms of the specific contract'.[1012] The effect of those doctrines in Australian law is not significantly different,[1013] and the attributes and interactions of eObjects do not in this context add anything substantial to Mik's analysis.

3.5.4.3 Undue influence

Mik also discussed undue influence in the context of digital consumer manipulation enabled by 'conventional' online contracting. However, Mik's discussion is unfortunately not very useful in the Australian context, as there are some significant divergences between Australian and UK law regarding undue influence.[1014] Eminent scholars and judges have argued that the undue influence doctrine in Australia has been effectively subsumed by equitable[1015] and statutory[1016] developments in unconscionable conduct. However, there is still some judicial and academic debate around the nature of the difference between undue influence and unconscionable conduct.[1017] Additionally, section 22(1)(d) of the ACL clearly states that 'undue influence' is a matter to

[1010] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42).

[1011] Ibid 28.

[1012] Ibid 29.

[1013] Carter, *Contract Law in Australia* (n 443) chs 20, 22.

[1014] Paul Finn, 'Common Law Divergences' (2013) 37 Melbourne University Law Review 509, 523–24.

[1015] Carter, *Contract Law in Australia* (n 443) [23-16]; Hardingham, 'Unconscionable Dealing' in PD Finn (ed), *Essays in Equity* (Law Book Co 1985) 17–19; Anthony Mason, 'The Place of Equity and Equitable Remedies in the Contemporary Common Law World' (1994) 110 Law Quarterly Review 238, 249.

[1016] *Berbatis* (n 925) [8].

[1017] *Amadio* (n 836) [2] (Mason J), [13] (Deane J); Carter, *Contract Law in Australia* (n 443) [23-16]; Peter Birks and Chin Nyuk Yin, 'On the Nature of Undue Influence' in Jack Beatson and Daniel Friedmann (eds), *Good Faith and Fault in Contract Law* (OUP 1995) 57, 59–60.

which the court may have regard when assessing whether conduct would be considered 'unconscionable' under section 21.

This area requires its own substantive exploration; that is beyond the scope of this dissertation, and only preliminary remarks are offered here. For example, one important question that remains unanswered is whether the concept of 'undue influence' under section 22 is the same as the 'unwritten law' doctrine of undue influence. This is important as there are significant constraints on the traditional doctrine, which are briefly discussed below. However, this dissertation recognises that these constraints may not be reflected in actions brought under the broader frame of unconscionable conduct under section 21 of the ACL. This is of practical relevance, as plaintiff consumers have substantial strategic reasons to rely on section 21 claims rather than equitable actions of undue influence.

The traditional Australian 'unwritten law' doctrine of undue influence is based on the protection of:

> a person who has entered into a transaction without a genuine consent in the sense that the court is satisfied, whether by evidence of actual undue influence or by a presumption arising from a special relationship of influence, that the transaction was not the result of an independent exercise of judgment.[1018]

In circumstances where actual influence[1019] cannot be shown, Australian law has traditionally required a relationship of 'trust and confidence',[1020] or at least 'a position … involving an ascendancy or influence over [an]other'.[1021] Where such a relationship exists, the law creates a rebuttable presumption that a transaction between the parties is the result of undue influence by the ascendant party.[1022] The transaction need not even be disadvantageous to the

[1018] LexisNexis, *Halsbury's Laws of Australia (online)* (LexisNexis 2013) [35.8.280].

[1019] See *Louth v Diprose* [1992] HCA 61 for an example of *actual* influence.

[1020] *Johnson v Buttress* [1936] HCA 41; (1936) 56 CLR 113, 119.

[1021] Ibid 135.

[1022] Michael Evans and Bradley Jones, *Equity and Trusts* (LexisNexis Butterworths 2012) [15.1].

influenced party, although proof of adequate consideration or independent advice for the transaction can be submitted to rebut the presumption.[1023]

In evaluating whether a relationship is one that leads to a presumption of undue influence, or in proving that actual undue influence occurred, courts have confined themselves to the evaluation of person-to-person relationships. However, the emergence of new eObjects and systems may create new categories of relationships with elements of trust and confidence, like those made with other human beings. The use of a digital personal assistant such as Max, or a doll such as Ella, provides a couple of scenarios where consumers may rely on a 'relationship' of trust and confidence to the extent that they take advice about the suitability of particular purchases or actions.[1024] Some more significant relationships of dependency may also arise in areas such as the use of autonomous or semi-autonomous robots for in-home aged care.[1025]

Academic commentary on whether 'intelligent' or 'autonomous' agents *should* be considered persons has recently seen a revival, most likely due to substantial publicity surrounding developments in artificial intelligence technologies.[1026] How judges will deal with these situations is currently unknown. Aside from the normative question, Australian judges are unlikely to hold that *current* law recognises a relevant relationship with an eObject, however anthropomorphised they may be in the consumer's mind. This would require the development of a whole new category of legal person,

[1023] Ibid [15.20], [15.21].

[1024] Stucke and Ezrachi, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' (n 803); Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (n 172).

[1025] See for example, Sophia Bolden, 'Personal Robots Helping Elderly in Their Homes' (*Telstra iCareHealth,* 9 November 2015) <www.icarehealth.com.au/blog/personal-robots-helping-elderly-in-their-homes/> accessed 29 January 2018.

[1026] Sartor, 'Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents' (n 354); Čerka, Grigienė and Sirbikytė, 'Is It Possible to Grant Legal Personality to Artificial Intelligence Software Systems?' (n 354); Laukyte, 'Artificial Agents Among Us: Should We Recognize Them As Agents Proper?' (n 354); Vladeck, 'Machines Without Principals: Liability Rules and Artificial Intelligence' (n 156).

something that is likely to be deferred to the legislature. More likely in appropriate cases is the judicial recognition of a relationship of trust and confidence with the legal person or persons providing Max's underlying services. However, there is also the possibility that judges may find that *no* relevant relationship exists.

4 REGULATORY DISCONNECTION ARISING OUT OF DIGITAL CONSUMER MANIPULATION

The analysis above has uncovered significant regulatory disconnection between the existing law and sociotechnical change brought about by eObjects in the area of digital consumer manipulation. Two specific 'legal problems' (from the categories of legal problems set out in **section 2.2.1.2** of **Chapter 3**) have been identified.

The first problem is **uncertainty,** specifically the uncertainty brought about by the lack of definition and coherent principle underlying the term 'unconscionable conduct', as discussed in **section 3.3** of this chapter. The dissertation proposes that a second legal problem also arises in relation to digital consumer manipulation enabled by eObjects. A systemic lack of transparency and a culture of secrecy in corporate dealings with consumer information potentially creates a '**new harm**' affecting consumers who buy and interact with eObjects.

These two legal problems are discussed further in this section below.

4.1 Uncertainty

> I don't know how I can decipher where my data goes and how it's used. It concerns me, but it's not transparent to me.[1027]

The legal problem of uncertainty uncovered by application of the ACL provisions to digital consumer manipulation enabled by eObjects provides a

[1027] Anonymous focus group respondent in focus groups run by Roy Morgan Research on behalf of the Consumer Policy Research Centre: Nguyen and Solomon, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (n 646) 28.

specific example of one of the pitfalls of technological neutrality discussed in general terms in **section 2.2.1.3** of **Chapter 3.** The ACL provisions most likely to be called into action by consumers and regulators to offset harms brought about by digital consumer manipulation enabled by eObjects are technologically neutral. This may lead people to the conclusion that the provisions are broad enough and flexible enough to accommodate emerging technologies, and this is a common argument provided by those advocating broadly-drafted 'neutral' provisions.[1028] However, the analysis in **Chapter 6** has shown that while some forms of digital consumer manipulation may be caught, the wording of the provisions is so general that their application is *uncertain*, and therefore may fail to protect consumers from many harms caused by digital consumer manipulation.

This dissertation argues that the ACL's unconscionable conduct provisions on their face *should* have provided a useful tool to protect consumers from unfair tactics and exploitation of consumer vulnerabilities. However, the uncertainty engendered by overly broad drafting and unhelpful case law has provided little guidance to business, consumers and regulators. This provides a strong disincentive to both proactive good practice by business and the likelihood of enforcement actions by both consumers and regulators.

4.2 A lack of transparency – a 'new harm'?

Negative effects of uncertainty are likely to be exacerbated by corporate secrecy and other forms of opaqueness. It is generally known that commercial entities and their third-party contractors conduct a large amount of experimentation on consumer responses to the digital environment, but this is kept confidential.[1029] This makes the specific details of the experiments and their results difficult to come by.[1030] There is no incentive – rather the opposite – for service providers and marketers to

[1028] See in particular nn 369–372 for literature discussing the foundations of support of the technological neutrality principle.

[1029] Nadler and McGuigan, 'An Impulse To Exploit: The Behavioral Turn in Data-Driven Marketing' (n 647) 156.

[1030] Ibid.

disclose to consumers or regulators the full extent of the data collected and used, or the nature of the cognitive biases or vulnerabilities they choose to attempt to exploit. Suppliers unsurprisingly favour vague, broad and generic privacy policies. There are some circumstances where suppliers have ostensibly attempted to provide more information. For example, some social media sites have a section titled 'Why am I seeing this ad?'[1031] However, empirical research has found this information to be 'incomplete', 'misleading' and 'vague'.[1032] It is counterproductive for service providers to disclose to consumers when and how they use digital consumer manipulation techniques. This is because it may reduce the techniques' effectiveness[1033] (although this does not always occur)[1034] and/or cause reputational damage due to a consumer backlash. The employment and job descriptions of behavioural psychologists, and algorithm writers, is not something most suppliers will willingly reveal to consumers. The very design of such techniques is intended to preclude self-discovery by consumers.

Without a working understanding of the data collected, the inferences drawn from that data, and what companies know about the effects of behavioural advertising, there is every chance that consumers will not realise what has actually happened to them, other than experiencing a case of buyer's remorse. They will ask themselves the question 'why did I do something so irrational or so harmful?' without having any idea that someone is to blame other than themselves.

The lack of transparency of digital consumer manipulation techniques is just one example of the issues that have recently arisen around market and algorithmic transparency. (The term 'transparency' here is used in its normal

[1031] For example, Facebook and Twitter, as at 30 June 2018.

[1032] Athanasios Andreou and others, 'Investigating Ad Transparency Mechanisms In Social Media: A Case Study of Facebook's Explanations' (Network and Distributed Systems Security (NDSS) Symposium 2018, San Diego, February 2018) 1.

[1033] Mik, 'The Erosion of Autonomy in Online Consumer Transactions' (n 42) 8.

[1034] Nadler and McGuigan, 'An Impulse To Exploit: The Behavioral Turn in Data-Driven Marketing' (n 647) 160.

English language sense of 'open to public scrutiny', or 'easily seen through or understood'.[1035] In some computing contexts, 'transparency' means rather the opposite.[1036]) Pasquale has sketched out other possible detrimental consequences of the growing collection of data by corporate actors, where use and abuse is screened from data subjects' view due to permitted corporate secrecy practices.[1037] Other scholars have delineated problems in state use of data and algorithms, for example in policing contexts.[1038] In Europe, legislators have recognised the need to address the problems that a lack of transparency can bring, such as inappropriate discrimination in decision-making by algorithms. As a result, the EU's new General Data Protection Regulation[1039] attempts to restrict some forms of automated individual decision-making, including a 'right to explanation' of algorithmic decisions.[1040] However, the efficacy of this attempt has already been doubted.[1041] It may foster instead a 'transparency fallacy', where 'transparency may at best be neither a necessary nor sufficient condition for accountability and at worst something that fobs off data subjects with a remedy of little practical use'.[1042]

As the use of data analytics increases, and transparency decreases, the likelihood of disbenefits for consumers and other data subjects is likely to increase. This type of lack of transparency falls into the category of a 'new

[1035] Butler, *Macquarie Dictionary: Australia's National Dictionary Online* (n 5).

[1036] Manwaring and Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (n 84) 591.

[1037] Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (n 144).

[1038] For example, Peeters and Schuilenburg, 'Machine Justice: Governing Security through the Bureaucracy of Algorithms' (n 701).

[1039] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

[1040] Ibid art 22.

[1041] Edwards and Veale, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking for' (n 704); Sandra Wachter, Brent Mittelstadt and Luciano Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.

[1042] Edwards and Veale, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking for' (n 704) 43.

harm' type of legal problem (as discussed in **section 2.2.1.2** of **Chapter 3**). The new activities now made possible by the eObjects' attributes, particularly hyper-personalised profiling, and algorithmic microtargeting of marketing campaigns, may lead to an opaqueness unprecedented in the consumer space: in other words, a mass inability to know our own minds.

5 CONCLUDING REMARKS

This chapter has examined the state of the law in relation to the challenge of digital consumer manipulation. Its detailed doctrinal examination of the law has uncovered legal problems in two categories outlined in **section 2.2.1.2** of **Chapter 3**, namely uncertainty and the existence of new harms. However, it appears that not all of this regulatory disconnection, particularly in the area of uncertainty, has been brought about solely by the sociotechnical change under examination. The examination has also revealed 'old' problems with the ACL that are exacerbated and revealed anew by the advent of eObjects and the systems in which they participate.

Chapter 7 outlines and outlines some potential changes in legal approaches necessary to address the legal problems identified in relation to digital consumer manipulation enabled by eObjects. While a full proposal of law reform is not possible within the frame of this dissertation, this exercise is nevertheless important in laying a solid foundation for any process of regulatory 'reconnection', that is, to close the gap between existing law and this form of sociotechnical change so as to achieve, or at least significantly reduce the conflict with, the Consumer Goals.

Chapter 7 – Kickstarting reconnection

1 AIMS OF CHAPTER

The in-depth doctrinal analysis of digital consumer manipulation discussed in **Chapter 6** identified significant regulatory disconnection between existing consumer law and the sociotechnical change brought about by eObjects. **Chapter 6** identified two legal problems that exist in relation to digital consumer manipulation enhanced by eObjects. First, there is uncertainty based on the unhelpfulness of overly general legislative drafting and a judicial approach which favours flexibility over certainty of principle. Second, there is a new harm effected by the interaction between entrenched

corporate secrecy practices, a consequential lack of transparency, and substantial 'dataveillance'[1043] by corporate actors.

Employing a mechanism to uncover legal problems is a significant step in dealing with regulatory disconnection in the face of sociotechnical change, but it is only a beginning. Further work needs to be done in establishing what can be done to 'reconnect' the law with the new things, activities and relationships brought about by new technologies. This dissertation does not attempt to provide a detailed proposal on law reform, as the *frame* of this dissertation precludes such a significant undertaking. However, as the next step towards this type of reform, this chapter proposes in broad terms the basic principles and some of the major features that legal frameworks should adopt in any attempt to move the existing law closer to achieving the relevant **Consumer Goals**.

2 RECONNECTING THE LAW TO A CHANGING SOCIOTECHNICAL LANDSCAPE

As discussed in **section 4** of **Chapter 6**, the in-depth doctrinal study conducted in this dissertation went on to establish the existence of two legal problems in the area of eObjects and consumer protection: first, uncertainty, and second, the existence of a 'new harm', that arising from a lack of transparency in terms of corporate conduct.

2.1 What areas of DCM should be regulated?

The broad analysis undertaken in **section 3.3.1** of **Chapter 5** established that digital consumer manipulation enabled or facilitated by eObjects could potentially cause outcomes that conflict with the **Consumer Goals** of **Fairness**, (avoiding) **Disadvantage**, and **Choice**. However, potential conflict with these goals does not automatically imply that all forms of digital consumer manipulation must be prohibited, as the interests of businesses and the economy in general also need to be taken into account. No clear societal consensus has been revealed as to exactly what sort of

[1043] Roger Clarke, 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498.

digital consumer manipulation *is* unacceptable, and this needs to be established before real reform is undertaken. However, some initial guidance can be taken from the ACCC's recent analysis of a number of empirical surveys taken of Australian consumers, as discussed in its Digital Platforms Inquiry final report.[1044] This analysis revealed that a significant majority of Australian consumers are opposed to:

1) tracking of location data;

2) online tracking for targeted advertising; and

3) sharing of data with unknown third parties;

in many circumstances.[1045]

These surveys were not undertaken in the specific context of eObjects, but rather digital platforms such as Google and Facebook, but it can be argued that the addition of eObjects into the process makes consumer harm in all three areas more likely. In particular, eObjects attributes such as **associability**, **mobility**, **geolocatability** and **prevalence** can all add to the amount and perceived quality (for example more frequent, timely and precise data points) of the datasets prized by corporates in the first two areas. This 'better data' can also increase the value to third parties, thereby encouraging data transfer by the initial collectors of the data.

Further empirical research on these areas is warranted however, as to what exactly it is about digital consumer manipulation is not acceptable by society to the extent it should be restricted in some way by the law. *Some* form of attempted influence by sellers has been a normal part of commercial life for many years, and additionally businesses argue that data collection and transfer is vital to minimising costs to consumers. Therefore, very broad prohibitions of any form of digital consumer manipulation are both unrealistic and likely unwarranted. It is as yet unclear what types of conduct would be most harmful to consumers. Is it personalised pricing? Is it other

[1044] Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (n 82).
[1045] Ibid Ch 7.

forms of discrimination? Is it searches for and specific targeting of known vulnerabilities? Is it attempts to *create* vulnerabilities?[1046] Are there particular cognitive biases that society generally agrees should not be exploited, while others are fair game for advertisers? All of these areas are worth investigating, but the most urgent questions arise in relation to the Consumer Goal of avoiding **Disadvantage**: that is, attempts to manipulate *vulnerable and disadvantaged groups*, for example children, people with disabilities, the elderly, people with mental health issues, the uneducated, people on low incomes and people with addictions.

Empirical research on attitudes of, and effects on, consumers and other interest groups is warranted, but this research can valuably be informed by combining it with other approaches. For example, European researchers Sax, Helberger and Bol[1047] recently took an interdisciplinary approach (combining ethics, communication and legal approaches) to dealing with the acceptability (or otherwise) of selling commercial products through mobile health applications. As their basis, the researchers identified that the fundamental goal of European rules regulating unfair commercial practices was the protection of autonomy. They then investigated the ways that the health apps attempted to influence users, formulated three requirements for autonomy based on ethics scholarship, conducted empirical research into both user attitudes and actual effects on users, and developed a framework for evaluating commercial practices against the autonomy requirements. A similar approach applied to consumer challenges under Australian laws may be beneficial.

2.2 Existing approaches and their limitations

Once some form of consensus is reached on the types of digital consumer manipulation that are and are not unacceptable, a sensible next step would be to investigate appropriate ways to 'fix' these problems. A standard response would then be to suggest amendments or additions to the ACL to

[1046] If created vulnerabilities are to be regulated, corresponding amendment of the relevant Consumer Goal of avoiding Disadvantage would also be recommended, in order to clarify that it was not restricted to those with pre-existing vulnerabilities.

[1047] Sax, Helberger and Bol, 'Health As a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices' (n 805).

respond directly to the undesirable conduct. However, any attempt at law reform should not be undertaken in isolation, but considered in the context of what is known (and what is not yet known) about sociotechnical change, and its amenability to regulatory reconnection. Additionally, further research is needed on the efficacy of existing mechanisms for law reform in the context of sociotechnical change.

Common approaches suggested by business and other non-consumer stakeholders include:

1. The use of test cases;
2. The use of non-enforceable regulatory guidance material; and
3. The provision of services based on a disclosure and consent model, where ostensibly the consumer is provided with sufficient details to understand the benefits and harms of the goods or services offered, and has the choice whether to accept or reject the terms of purchase.

However, all of these approaches have significant limitations.

2.2.1 Test cases

The uncertainty of the unconscionable conduct provisions is not confined to digital consumer manipulation. It is not a 'new' problem. However, the negative effects of uncertainty may be greater in the context of sociotechnical change compared to other forms of social change, due to the speed and complexity of change. Various parliamentary inquiries have suggested that the specificity craved by consumers and small business groups could be dealt with by the regulator running test cases, rather than facing the administrative burden of providing examples within the legislation that must be continually updated. They have also suggested the use of guidance material by the ACCC. However, a number of problems arise from these suggestions in the context of sociotechnical change, particularly around effective regulatory timing (as discussed in **section 2.2.3** of **Chapter 3**).

First, the judicial process invoked in running test cases has many problems, although only two will be mentioned here. Despite all of the attention given

in recent years to efficient case management, litigation remains very slow[1048] and expensive. Consumers do have recourse to small claims tribunals for breaches of the ACL,[1049] where proceedings are quicker and cheaper, but these decisions have limited precedent value, particularly as some tribunal members are not required to be legally qualified.[1050] Substantive litigation is usually beyond the resources of ordinary consumers, and often regulators as well. As discussed above, it has not previously produced useful general principles easily applied or understood by businesses planning to engage in, or consumers faced with, *different* conduct. If useful cases are produced too slowly, or not at all, then society ends up on the side of the Collingridge dilemma (discussed in **section 2.2.3** of **Chapter 3**) where it may be too late to mitigate harms because of entrenched interests. Judges have previously accepted arguments that conduct that is 'normal' or 'ordinary' business practice should not be considered unconscionable[1051] (although this is not necessarily determinative). Therefore, conduct left unchecked for too long may create its own legitimacy, to the detriment of consumers and others.

2.2.2 Guidance material

The use of guidance material as a substitute for stronger regulation has also been subject to criticism. Cortez recently undertook a case study of two contrasting types of regulatory processes in the US to regulating emerging

[1048] Even judges – or at least former judges – acknowledge this: '[t]he whole system is rotten with excessive delay': JD Heydon, *Does Political Criticism of Judges Damage Judicial Independence?* (Policy Exchange Judicial Power Project Paper, February 2018) 16.

[1049] The ACT Civil and Administrative Tribunal, the New South Wales Civil and Administrative Tribunal, the Northern Territory Civil and Administrative Tribunal, the Queensland Civil and Administrative Tribunal, the South Australia Magistrates Court, the Magistrates Court of Tasmania, the Victorian Civil and Administrative Tribunal, and the Magistrates Court of Western Australia. Australian Competition and Consumer Commission, Small Claims Tribunals <https://www.accc.gov.au/contact-us/other-helpful-agencies/small-claims-tribunals> accessed 12 May 2019.

[1050] For example, in New South Wales: Civil and Administrative Tribunal Act 2013 No 2 (NSW) s 13.

[1051] For example, *Australian Competition and Consumer Commission v Woolworths Ltd* [2016] FCA 1472.

technologies. He concluded that mere guidance by regulators without follow-up regulation and enforcement may lead to a calcification into a 'weak default position'.[1052] He argues that a 'regulatory threat works best as a temporary stopgap that presages more traditional regulatory intervention, not as a long-term strategy.'[1053] This study was done in a US regulatory context and therefore the results cannot be applied without caution in the Australian regulatory landscape. However, Cortez's study does raise concerns that should be addressed. In particular, to what extent can the preservation of 'flexibility' as the dominant factor in making decisions about regulation – and vaunted as a virtue in the cases on unconscionable conduct – lead to 'legal procrastination'[1054] and a 'regulatory inertia'?[1055] This question is particularly significant as Cortez argues that such inertia is difficult to break without a significant and public failure.

2.2.3 Disclosure and consent models

The effectiveness of disclosure and consent models in preventing harm to consumers faced with standard-form contracts and mass collection, processing and transfer of data have been robustly challenged.[1056] Disclosure by businesses to consumers is often very light on useful detail, consumers can be overwhelmed by the volume and unintelligibility of material, access to appropriate disclosure can be difficult to navigate, and in Australia at

[1052] Nathan Cortez, 'Regulating Disruptive Innovation' (2014) 29 Berkeley Technology Law Journal 175, 227. See also John Braithwaite, 'Responsive Regulation and Developing Economies' (2006) 34 World Development 884, 888, 'where in practice enforcement is spread around thinly and weakly … [h]ardened offenders learn that the odds of serious punishment are low for any particular infraction'. Cf Tim Wu, 'Agency Threats' (2011) 60 Duke Law Journal 1841, 1848–54.

[1053] Cortez, 'Regulating Disruptive Innovation' (n 1052) 179.

[1054] David A Super, 'Against Flexibility' (2011) 96 Cornell Law Review 1375, 1382. See also the discussion of 'retreatism' by regulatory agencies in Robert A Kagan, 'Understanding Regulatory Enforcement' (1989) 11 Law & Policy 89, 93.

[1055] Cortez, 'Regulating Disruptive Innovation' (n 1052) 202.

[1056] For example, Omri Ben-Shahar and Carl E Schneider, *More Than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton UP 2014); Elena D'Agostino, *Contracts of Adhesion Between Law and Economics: Rethinking the Unconscionability Doctrine* (Springer 2015) 50; Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (n 82) 394-422, 449-51.

least, consumers do not perceive consent mechanisms as being protective of them.[1057] The lack of effectiveness may actually be worse in the context of digital consumer manipulation, as some scholars recognise that the nature of behavioural advertising tactics is such that they 'may not be able to be defused by raising users' awareness or knowledge of how they operate.'[1058]

However, there are other approaches to disclosure that may assist. Better targeting and framing of disclosure are tactics that should be investigated for their potential for increased effectiveness. For example, on 9 April 2019 a bipartisan bill was introduced to the US Senate called 'Deceptive Experiences to Online Users Reduction Act' (**DETOUR Bill**).[1059] It is not directed at digital consumer manipulation enabled by eObjects, but targets similar types of behaviour undertaken online. The bill is intended to 'prohibit the usage of exploitative and deceptive practices by large online operators and to promote consumer welfare in the use of behavioral research by such providers'.[1060] Part of the DETOUR Bill mandates:

1. regular disclosure to users and to the public of any behavioural or psychological research undertaken for 'the purpose of promoting engagement or product conversion';[1061] and

2. the appointment of an Independent Review Board registered with the FTC for each operator, whose purpose is to oversee any behavioural or psychological research conducted by large online operators.[1062]

The first of these is a powerful provision. However, the likelihood of it passing into law is not high, due to its effect on businesses and the forced disclosure to competitors of confidential information that exists to foster a

[1057] See for example Nguyen and Solomon, *Consumer data and the digital economy: emerging issues in data collection, use and sharing* (n 646).

[1058] Nadler and McGuigan, 'An Impulse To Exploit: The Behavioral Turn in Data-Driven Marketing' (n 647) 160.

[1059] S. 1084, 116th Congress (2019).

[1060] S. 1084, 116th Congress (2019), § 1.

[1061] S. 1084, 116th Congress (2019), § 3(b)(1)-(3).

[1062] S. 1084, 116th Congress (2019), §§ 3(b)(4)-(5).

competitive advantage. There are also other shortcomings, at least when considered in an Australian context, that might fail to protect consumers as intended. First, there remains a question as to competency and power of the proposed disclosees to act appropriately on such disclosure, and second, whether simply the nature of the research constitutes sufficient disclosure to readily avoid harm. Additionally, there is the question of whether supposedly independent review boards paid for by the operators will devolve into mere 'ethics-washing' or 'ethics-shopping' exercises.[1063]

A preferred alternative scheme could provide for detailed and specific disclosure of *use* of data, *inferences* made from that data, and the nature of *behavioural research* undertaken, commissioned or used by corporates. However, in order to overcome some of the objections of non-consumer stakeholders, this disclosure could be made commercial-in-confidence (to prevent a contested disclosure of trade secrets) to an educated *regulator* or other agency[1064] with a remit to investigate the desirability or appropriateness of particular conduct. This approach may be more fruitful in preventing serious harms to consumers while still balancing an interest in robust competition.

Robust disclosure mechanisms are important to assist in overcoming the problems of corporate secrecy identified in **section 4.2** of **Chapter 6.** However, disclosure and consent mechanisms *on their own* are likely to be insufficient in protecting consumers against real harms, particularly in light of the significant limitations on consent discussed in s**ections 3.5.1** and **3.5.3** of **Chapter 6**. As discussed in **section 3.5.3** of **Chapter 6**, one of the strengths of Australian consumer protection law is in its recognition that consumers in some circumstances need to be protected against seller misconduct even when they have ostensibly 'consented' to a transaction.

[1063] Ben Wagner, 'Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?', in Emre Bayamlioglu and others (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press, 2018).

[1064] Daniel J Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880, 1802.

2.3 The regulation of conduct and the need for swifter legal responses to sociotechnical change

Considering the limitations of disclosure and consent models, the value of specific regulation targeting inappropriate *conduct*, such as particular forms of behavioural advertising, or inappropriate recommendations, should be explored. Such a response could be narrowly targeted, such as in the case of the door-to-door selling regime in the ACL, which is helpful in that it recognises that a particular form of conduct is likely to lead to a type of 'situational vulnerability',[1065] that cannot be overcome by ostensible 'consent' at the moment of sale. However, the limitations to this approach have already been discussed in **section 3.4** of **Chapter 6**.

A further examination of the proposed US DETOUR Bill (discussed at **section 2.2.3** of this chapter) may assist. The DETOUR Bill, in addition to its disclosure and consent provisions, also purports to prohibit:

- 'user interface design' that:
    - obscures, subverts or impairs 'user autonomy, decision-making, or choice to obtain consent or user data'[1066] and,
    - in the case of children under 13, 'cultivat[es] compulsive usage'.[1067] 'Compulsive usage' is defined as

        > any response stimulated by external factors that causes an individual to engage in repetitive, purposeful, and intentional behavio[u]r causing psychological distress, loss of control, anxiety, depression, or harmful stress responses;[1068] and

- dividing consumers into groups for 'behavio[u]ral or psychological experiments or studies' without informed consent.[1069]

[1065] Productivity Commission, *Review of Australia's Consumer Policy Framework* (n 420) vol 2, 13.
[1066] S. 1084, 116th Congress (2019), § 3(a)(1)(A).
[1067] S. 1084, 116th Congress (2019), § 3(a)(1)(C).
[1068] S. 1084, 116th Congress (2019), § 2(3).
[1069] S. 1084, 116th Congress (2019), § 3(a)(1)(B).

However, narrowly targeted and/or technologically specific changes to legislation such as this can quickly become out-of-date. For example, the drafting of the DETOUR Bill, with its emphasis on 'user interface design' may be appropriate for website menus, but may not apply to manipulation undertaken in other ways by eObjects, such as on time of day, location, proximity to certain other individuals or blood sugar levels, or systems that rely for their manipulative effect on a *number* of separate parties and 'interfaces'. It is also solely directed at large 'online' operators, which fails to take into account the complexities of the provider network underlying many eObjects and the systems in which they participate.

Examination of more expansive and consumer-focussed general legislative regimes may also be worthwhile, such as the 'unfair conduct' prohibition in the US.[1070] However, the analysis of unconscionable conduct and digital consumer manipulation in **Chapter 6** provides some evidence for the general contention that 'technologically neutral' legislation, even when combined with the 'flexibility' of a common law precedent system, is not adequate to address many problems of regulatory disconnection and reconnection in the face of sociotechnical change. So, the adoption of a general 'unfair conduct' approach, without more, may be insufficient to deal with this problem.

When sociotechnical change occurs, legislatures, courts, and doctrinal scholars tend to rely heavily on judicial interpretation of existing common law and legislative principles, at least those that are prima facie 'technologically neutral'. This approach is often preferred because it:

- is less conceptually challenging than a *sui generis* approach;[1071]
- sits more comfortably with a common law system; and

[1070] 15 USC § 45.

[1071] For a discussion of the benefits and risks of *sui generis* rules in dealing with sociotechnical change, see Lyria Bennett Moses, 'Sui Generis Rules', in Marchant, Allenby and Herkert (eds), *Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem* (n 18) 77 - 94.

- does not single out particular sectors for special treatment.

Development of specific principles from very general statutory formulations is left up to the judiciary, because, as argued by a senior Australian judge, this 'is a task at the very heart of the judicial process'.[1072] However, there are a number of limitations with this approach in the context of sociotechnical change that are worth investigating.

Cockfield has criticised traditional legal analysis as 'incomplete' in the context of sociotechnical change, and has urged a more 'liberal' approach, including a flexible approach to interpretation, that incorporates policy considerations when faced with sociotechnical change that 'may affect important interests and values'.[1073] Judicial interpretation of statutory principles is an essential part of the process of law 'keeping up' with sociotechnical change. However, it is not a complete substitute for necessary and active intervention by legislative and regulatory authorities.

Problems arising from a lack of *ex ante* guidance as to what constitutes acceptable business conduct in a rapidly changing environment were discussed in **Chapter 6.** Additionally, as discussed in **section 2.2.1.3** of **Chapter 3**, the question arises as to whether attempts to continually expand the interpretation of general legal principles to emerging sectors, where those principles emerged in reaction to a vastly different context, can have the effect of overstretching existing doctrines beyond manageability or sense. This is one danger inherent in Cockfield's approach. In relation to eObjects, a similar risk exists in that overly strained interpretations of common law principles or broad statutory provisions designed for a significantly different sociotechnical landscape may in their turn lead to doctrinal distortion and subsequent degradation of relevant norms.

Rigid adherence to a principle at one end of the spectrum (technological neutrality) or at the other (technological specificity) may be less effective than adoption of a principle of technological *appropriateness* in the

[1072] *CBA v Kojic* (n 915) per Allsop CJ [58].

[1073] Cockfield, 'Towards a Law and Technology Theory' (n 319) 384.

development and application of legal rules by legislative drafters and judges in the face of sociotechnical change.

However, any introduced principle of technological appropriateness would of course face a significant challenge around an appropriately *timed* response to sociotechnical change. It is essential that any framework must consider mechanisms for swifter responses by legislators and regulators, in forms amenable to quick review and assessment to keep the response up to date.

Any solution must then deal with the too general/too specific problem, and the timing problem. One possible solution that may have some merit could include a structure along the lines of:

1. a general prohibition supported by a 'blacklist', or examples of specific unfair conduct (such as seen in Annex I to the EU provisions on 'unfair commercial practices'[1074], or the specific examples of unfair contract terms provided in section 25 of the ACL); **PLUS**

2. the use of rule-making capabilities by regulators to make changes to the blacklist (such as those proposed by the ACCC in relation to the CDR[1075]); **PLUS**

3. enforced disclosure of corporate practices (as discussed in **section 2.3** of this chapter).

The 'blacklist' could include, if the societal consensus discussed in **section 2.1** of this Chapter dictates, specific examples of conduct by suppliers that has the effect or purpose of impairing a consumer's autonomy or decision-making capabilities, or attempts to exploit or create a particular vulnerability.

This solution constitutes one avenue of promise in speeding up responses to sociotechnical change in general, and manipulative practices specifically. The

[1074] Unfair Commercial Practices Directive (EU) (n 831).
[1075] See discussion in **section 3.4.1**, **Chapter 5**.

legislative provisions could provide as much *ex ante* guidance as is practically possible, and the disclosure of new corporate practices as they emerge could be responded to more quickly under rule-making capabilities of regulators. As an alternative to direct changes to the ACL, co-regulatory initiatives[1076] such as statutory Codes of practice may also be helpful, at least where the views of stakeholders beyond industry and government are appropriately integrated.[1077]

The use of technology assessment panels or specialist agencies to assist regulators in this exercise or to act as stand-alone review panels (possibly with a 'stop-and-review'[1078] power) for new uses of technology or data may also assist.[1079] The utility of such bodies would also be assisted where they are granted power to compel detailed disclosure by individual corporate entities of their confidential practices. On 9 March 2019, the House of Lords Select Committee on Communications recommended the establishment of a 'Digital Authority' in the UK that would have the following functions (amongst others):

> – to continually assess regulation in the digital world and make recommendations on where additional powers are necessary to fill gaps;
> – to establish an internal centre of expertise on digital trends which helps to scan the horizon for emerging risks and gaps in regulation;
> – to help regulators to implement the law effectively and in the public interest…;

[1076] Australian Communications and Media Authority, *Optimal Conditions for Effective Self- and Co-regulatory Arrangements* (Occasional Paper, June 2015) 10–11; Australia, Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation* (March 2014) 28.

[1077] Roger Clarke and Lyria Bennett Moses, 'The Regulation of Civilian Drones' Impacts on Public Safety' (2014) 30 Computer Law and Security Review 263, 278.

[1078] Derek Morgan, 'Technology in the Age of Anxiety: The Moral Economy of Regulation' (2009) 29 Legal Studies 492, 508.

[1079] Solove, 'Introduction: Privacy Self-Management and the Consent Dilemma' (n 1064) 1902; Brownsword, *Rights, Regulation, and the Technological Revolution* (n 39) 288–90; Greenberg, 'Rethinking Technology Neutrality' (n 370) 1547; Bennett Moses, 'Regulating in the Face of Sociotechnical Change' (n 330) 590–91.

- to inform Parliament, the Government and public bodies of technological developments;
- to provide a pool of expert investigators to be consulted by regulators for specific investigations;
- to survey the public to identify how their attitudes to technology change over time, and to ensure that the concerns of the public are taken into account by regulators and policy-makers;
- to raise awareness of issues connected to the digital world among the public;
- to engage with the tech sector;
- to ensure that human rights and children's rights are upheld in the digital world.[1080]

The horizon-scanning,[1081] expertise location, and awareness-raising functions of such a body are likely to be helpful, although it is worthwhile to note that some of these functions are already allocated in the UK to bodies such as the Parliamentary Office of Science and Technology[1082] and the Centre for Data Ethics and Innovation.[1083] Australia has no such central body, but some of its functions are exercised, albeit usually ad hoc. For example, ACOLA is currently undertaking a horizon-scanning project entitled 'The Internet of Things: Maximising the benefit of deployment in Australia' requested by Australia's Chief Scientist, on behalf of the Commonwealth Science Council.[1084]

[1080] House of Lords Select Committee on Communications, *Regulating the Digital World* (2nd Report of Session 2017–19, HL Paper 299, 9 March 2019) [238]. Such a body is somewhat reminiscent of the now-defunct US Office of Technology Assessment.

[1081] See also David Rejeski, 'Public Policy on the Technological Frontier' in Marchant, Allenby and Herkert (eds), *The Growing* Gap *Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem* (n 18) 51-53.

[1082] Parliamentary Office of Science and Technology <https://www.parliament.uk/post> accessed 9 May 2019.

[1083] Centre for Data Ethics and Innovation (CDEI) <https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei> accessed 9 May 2019.

[1084] Australian Council of Learned Academies (ACOLA), 'ACOLA Receives ARC Funding to Undertake Two New Horizon Scanning Projects on AI and IoT' (Media Release, 21 May 2018) <https://acola.org/artificial-intelligence-internet-of-things/>

2.4 Aiding consumer redress

Any solution must also account for the difficulties of achieving redress for consumers, and in particular problems of cost and speed of litigation. In contrast, the October 2018 proposal for an 'Office for Responsible Technology' by a private research organisation included an ombudsman-style service to assist in consumer redress.[1085] The ACCC also recommended an ombudsman scheme to deal with complaints about digital platform providers.[1086] This type of capacity is likely to be more useful for individual consumers than the expense and delay of formal litigation.

2.5 The role of the Privacy Act

As discussed in **section 3.5.1** of **Chapter 6** there are some significant and fundamental problems with the Privacy Act.[1087] Further research and policy development are urgently needed in this space, in two areas in particular. First, a comprehensive analysis of how the Privacy Act and the ACL interact in relation to the *use* of consumer data in the process of supplying goods and services is sorely needed.[1088] The ACCC Digital Platforms Inquiry was a welcome start to this process, but is confined in scope to digital platforms. The potential scope of the provider network in the context of eObjects is much wider, and may give rise to additional issues. The coverage of the

accessed 12 September 2019. The author of this dissertation has been briefed to provide an input report into this project.

[1085] Doteveryone, *Regulating for Responsible Technology – Capacity, Evidence and Redress: A New System for a Fairer Future* (October 2018) 6.

[1086] Recommendation 23, Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (n 82) 510.

[1087] Similar problems were outlined by the Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (n 82) ch 5, one week after the author's article containing this section was published.

[1088] In the UNSW Law School, a research project on application of the ACL provisions on unfair contract terms to privacy policies is currently well advanced: Email from Dr Katharine Kemp to dissertation author (20 November 2018). Additionally, in April 2019, a research grant from the International Association of Privacy Professionals – Australia/New Zealand Chapter Inc was awarded to UNSW researchers (including the author of this dissertation, Dr Rob Nicholls and Dr Katharine Kemp) for a project entitled '(mis)Informed Consent: Privacy, unfair contract and unconscionable conduct'. Letter from Melanie Marks to Rob Nicholls (18 April 2019).

Privacy Act, that is, the size of the businesses that are subject to its provisions, must also be considered,[1089] particularly considering the nature of the provider network for eObjects.

Second, following on from the above, an investigation and comparison of appropriate responsibilities, enforcement mechanisms and resources of the respective consumer protection and privacy regulators should be undertaken. This investigation is needed to ensure that important matters of consumer protection do not fall by assumption or default to a regulator that is underfunded, under-resourced and under-skilled in the protection of consumers.

The ACCC in its Digital Platforms Inquiry also made a number of recommendations that could assist in proper regulation of the harms brought about by digital consumer manipulation, and perhaps other data-based harms arising out of eObjects. The recommendations of most relevance to digital consumer manipulation include:

In the Privacy Act[1090]

1. **Recommendation 16(a):**
    - broader definition of 'personal information';
2. **Recommendation 16(c):**
    - The imposition of an *informed* consent requirement, in particular where collection, use or disclosure of the data is not necessary for the performance of a contract (or as a result of a legal or public interest reason); and
    - the introduction of default settings for consent that are pro-consumer and not bundled;

[1089] Recommendation 18, Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Final Report* (n 82) 476.

[1090] Ibid 456-496.

3. **Recommendation 16(e):**

    - a direct right of action for individuals;

4. **Recommendation 18:**

    - greater information requirements that align more closely to what consumers want to know, including a requirement that the name and contact details for each third party to whom personal information will be disclosed;
    - more sophisticated user control, including the use of personalised and global opt-in and opt-out controls; and
    - additional restrictions on children's personal information collected or used for targeted advertising or profiling purposes (note that the effectiveness (or otherwise) of pre-existing models in other jurisdictions, such as the Children's Online Privacy Protection Act of 1998[1091] (**COPPA**) in the US and the special protection offered to children under Articles 6, 8, 12, 57 and 40 of the GDPR should also be examined for this purpose.)

In the CCA[1092]

5. **Recommendation 21**: further prohibitions on unfair practices, including:

    - Collection or disclosure of consumer data without express informed consent;
    - Inducing consent by 'relying on long and complex contracts, or all or nothing click wrap consents, and providing insufficient time or information that would enable consumer to properly consider the contract terms'[1093]

[1091] 15 USC §§ 6501–6506.

[1092] Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (n 82) 498-501.

[1093] Recommendation 18, Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report* (n 82) 498.

All of these suggestions by the ACCC, however, are somewhat limited in their current form: as they are confined to digital platforms, and in their current wording are often too technologically specific to apply outside conventional online ecommerce to eObjects. For example, no attention is paid to the practical technical question of how user controls and consent would be managed when it comes to eObjects with form factors lacking a screen or other suitable interface.

Such substantive changes to the Privacy Act and the CCA are already considered contentious by businesses, and the operation of the Collingridge dilemma in relation to digital platforms can be seen in the responses by those with vested interests.[1094] Any road to reform will be long and contested. However, as a first step, stronger protections around the use of data for specific vulnerable or disadvantaged groups, such as children, those with disabilities, health problems or the elderly, should be considered as a matter of urgency.

3 CONCLUDING REMARKS

This chapter provided an outline of some of the major principles and features that any legal and regulatory framework must contain in any attempt to improve the existing law with an intent to remove existing conflicts with the **Consumer Goals**. When attempting to 'reconnect' a legal framework with the new things, activities and relationships brought about by new technologies, some of the common approaches to law reform may not be effective. Both technologically specific and technologically neutral approaches have their shortcomings. Additionally, traditional methods of

[1094] Eg Facebook, *Facebook's Response to the Digital Platforms Inquiry* (12 September 2019) 104-123, available at <https://fbnewsroomus.files.wordpress.com/2019/09/facebook-submission-to-treasury-on-digital-platforms-inquiry.pdf> accessed 15 September 2019; Digital Industry Group Inc, *ACCC Digital Platforms Inquiry Final Report: Submission to Treasury* (12 September 2019) 14-23, available at <https://digi.org.au/wp-content/uploads/2017/02/DIGI-ACCC-DPI-Submission-to-Treasury-12-September-2019-FINAL.pdf> accessed 18 September 2019. Digital Industry Group Inc founding members include Google, Facebook, Twitter, Verizon, Instagram, YouTube, Redbubble and Vodafone.

consumer protection, such as disclosure and consent models, have also proven ineffective in meeting consumer expectations in the face of sociotechnical change.

Chapter 6 identified two legal problems identified in as arising in the context of digital consumer manipulation. To address these, this **Chapter 7** proposed a principle of technological appropriateness may require the combination of a general and a specific approach to achieve the best type of reconnection. A general prohibition on unfair conduct could usefully be supplemented with a 'blacklist' of examples of prohibited conduct. However, this approach needs also to be combined with mechanisms for swifter responses to change, such as the use of rule-making capabilities by regulators and the use of swifter and more convenient consumer redress measures, to ensure that reconnection is to be sustained.

Experience in attempts at reform in the context of conventional online commerce have indicated that the pressure imposed by 'vested interests' as highlighted in the Collingridge dilemma is an ongoing problem. Therefore, urgent responses are needed, at least in relation to vulnerable and disadvantaged groups.

Chapter 8 concludes the dissertation. It summarises the dissertation's conclusions relating to the nature of the emerging technology at issue, the subsequent challenges for consumers, and the particular legal problems arising out of digital consumer manipulation. It reflects on the lessons learned during the enquiry. It also outlines implications for policymakers, which is very important in a fast-moving area. The chapter also outlines an agenda for further research relating to eObjects and the systems in which they participate.

Chapter 8 – Conclusion[1095]

1 AIMS OF CHAPTER

The aim of this enquiry was to explore the interaction between particular laws, those relating to consumer protection, and a particular technology, that of eObjects, by means of a broad and deep doctrinal examination. This

[1095] This chapter reproduces parts of a research paper published online and a journal article published during the course of doctoral study: Manwaring, 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (n 90); Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (n 2).

dissertation set out to seek answers to the following major research questions:

1) What types of sociotechnical change brought about by eObjects and the systems in which they participate will affect consumers?
2) To what extent do those types of sociotechnical change have the potential to hinder achievement of the goals of consumer protection law in Australia?
3) To what extent is there a gap between existing consumer protection laws and the goals they were intended to achieve in the context of digital consumer manipulation in which eObjects and related systems are involved in data collection and/or mediation of marketing messages?

The aim of this chapter is to summarise the dissertation's conclusions on these questions, to outline other key lessons learned from the enquiry, and to propose avenues for further research.

2 LESSONS LEARNED FROM THE ENQUIRY

In order to answer the major research questions posed in **Chapter 1**, this dissertation had to:

1) delineate the boundaries of the sociotechnical change at issue;
2) investigate the nature of the challenges that consumers confront in the face of that sociotechnical change; and
3) analyse the extent to which regulatory disconnection and legal problems exist in relation to one of the challenges identified, namely the challenge of digital consumer manipulation, and existing Australian law.

The first contribution of this dissertation was an extensive examination of the sociotechnical change arising out of the advent of eObjects. This was used in order to come to an understanding of the extent to which legal problems might arise in relation to Australian consumer protection law. The scope of sociotechnical change arising out of eObjects is substantial, so the research first took a broad approach to uncover particular challenges for consumers with detrimental outcomes that conflicted with the goals of Australian consumer protection law, leading to significant *potential* to give rise to legal problems. This was followed by an in-depth doctrinal analysis of

one of these challenges, that of digital consumer manipulation, in order to uncover *actual* legal problems. Proposed basic principles and general features of law reform aimed at addressing the actual legal problems identified were then outlined. A summary of the conclusions on these points is set out in **section 2.1** of this chapter.

A secondary (but nevertheless important) contribution of the primary enquiry was its usefulness as a case study to allow an assessment of the efficacy of a particular conceptual framework when applied to 'real-life' examples of emerging technologies. The conceptual framework was developed from emerging theories about how the interactions between law and technology should be conceived, and how research into legal problems arising from technological developments should be carried out. The execution of the primary research into the sociotechnical change arising from eObjects and subsequent challenges and legal problems, particularly the in-depth study of digital consumer manipulation enhanced by eObjects, has provided some insights into how that conceptual framework may be improved. Those insights are set out in **section 2.2** of this chapter.

2.1 eObjects

2.1.1 The sociotechnical change at issue

The world is facing significant sociotechnical change with the emergence of eObjects and the systems in which they participate. The investigation detailed in **Chapter 2** revealed that the nature of the technology underlying this change was ill-defined, with contradictory and overlapping uses of a range of terminology, particularly the terms ubiquitous computing, pervasive computing, ambient intelligence, and the Internet of Things. Definitions of these terms have varied depending on such factors as geographical locations and individual researchers, and have also changed over time.

Legal scholars, in particular, have not regularly engaged with a comprehensive and consistent view of the technology under discussion,

although there are exceptions to this.[1096] This failure has been understandable in relation to the discussion of emerging technologies at a general level of abstraction, and the challenges facing legal scholars in gaining a sufficient understanding of emerging and unstable technologies. However, if legal (and other) research is undertaken based on misunderstandings of technologies, substantial risks will arise. If a technology is not properly understood, one important consequence will be that the new things, conduct and relationships enabled by it will not be adequately mapped. Gaps and mistakes in understanding of both the technology and the sociotechnical change it enables will be detrimental to good policymaking and the discovery of regulatory disconnection in a timely manner. As discussed in **Chapter 3**, delay in uncovering gaps may lead to the entrenching of undesirable outcomes in the law due to the operation of the Collingridge dilemma. The dilemma concerns the appropriate timing of regulatory intervention, and its subsequent effectiveness. Interventions taken too early, that is before benefits and risks are clearly known, may lead to stifling of innovation and poorly targeted rules, while interventions taken later may be staunchly resisted by vested interests.

In order to overcome these problems, **Chapter 2** analysed the literature on historical and current definitions of the technologies under discussion. This analysis led to the formulation and definition of an original unifying concept for the technology under discussion, the 'eObject'. Since a simple definition cannot give a full picture of such a broad scope of technologies, **Chapter 2** also distinguished core and other attributes of the technology, as well as interactions among eObjects, other computing systems and devices, the physical world, and living things.

[1096] Most notably, Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (n 144). Postdating the author of this dissertation's article incorporating Chapter 2 of this dissertation, Manwaring and Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (n 84), articles dealing with definitional issues have included ; Millard, Hon and Singh, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (n 87); Mathews-Hunt, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (n 56).

The development of a definition of 'eObject', including its core attributes, and the identification of other attributes and interactions, provided a substantial technical research framework enabling this dissertation to analyse sociotechnical change arising from the technologies in relation to consumers, and the potential for legal problems arising as a result (discussed in the following sections). Additionally, this technical research framework provides a foundation for analysing the implications of this type of technology from legal, business strategy and policy perspectives outside the scope of this dissertation.

2.1.2 Challenges arising from the technology

As discussed in **Chapter 3**, identification of legal problems is crucial at an early stage of technological development, to assist in avoiding two problems. The first is the stifling of beneficial innovation by over-regulation. The second is the cementing of socially undesirable outcomes such the unlimited surveillance of private spaces, if vested interests are left unchecked. However, the fact that consumers may have challenges to face does not automatically imply that legal problems exist. Legislation or other rules may exist that have direct application to the new activities, things or relationships causing consumers concern.

Building on the foundation of the technical research framework developed in **Chapter 2**, **Chapter 4** provided a set of Vignettes. The purpose of these Vignettes was to outline some specific examples of sociotechnical change enabled by eObjects. These Vignettes showed how the attributes and interactions relating to eObjects identified in **Chapter 2** would impact the everyday life of consumers. They enabled the analysis of challenges and legal implications in subsequent chapters to be illustrated with realistic examples.

Chapter 5 of this dissertation identified (and, by use of the Vignettes, illustrated) a number of challenges for consumers in consumer transactions arising out of new things, activities and relationships made possible by eObjects. These challenges are numerous and varied, but can be categorised into five areas:

1) eObjects are imperfect;
2) eObjects can be controlled remotely by Providers;
3) eObjects can adversely affect consumer choice;
4) eObjects may have a significant post-supply value to Providers; and
5) eObjects are complex.

Detrimental outcomes of these challenges have the potential to conflict with the major goals of consumer protection law in Australia. Therefore, the challenges identified bear further investigation and analysis as to whether they are likely to give rise to legal problems in Australia (see discussion at **section 3.1** of this chapter). Similar potential for legal problems may also be found in jurisdictions outside Australia, as the goals of the current *United Nations Guidelines for Consumer Protection*[1097] are very similar to the goals of the ACL, and the *Guidelines* have a history of widespread adoption among UN member states.[1098] While the goals and therefore the *potential* for legal problems may be similar, the implementation of those goals into national legislation will vary widely, and therefore so will *actual*, rather than potential, legal problems. This divergence may in turn give rise to conflicts of law and jurisdiction issues, as well as forum shopping by business selling products and services related to eObjects.

While some of the challenges identified in **Chapter 5** are nascent, others have already caused problems for consumers, such as the exploitation of security vulnerabilities endemic in eObjects (see **section 3.1.1** of **Chapter 5**). Some have even formed the foundation of litigation in overseas jurisdictions, such as the 2016 class action against Standard Innovation (US) Corp alleging data collection of intimate personal information without consent (see **section 3.4.1.1** of **Chapter 5**). However, the challenges identified constitute more than mere inconveniences to consumers, such as is seen in the potential for physical harm inherent in the exploitation of security vulnerabilities in mobile eObjects (see **section 3.1.1** of **Chapter 5**).

[1097] United Nations Guidelines for Consumer Protection, GA Res 70/186, UN Doc A/RES/70/186 (adopted 22 December 2015).

[1098] Manwaring, 'Emerging Information Technologies: Challenges for Consumers' (n 95) 269.

Therefore, this dissertation lays a broad basis for further examination of consumer protection laws in Australia, in order to establish whether or not these challenges are currently addressed. Early literature on eObjects (and related technologies) made it clear that laws concerning consumer data protection and privacy need to be a priority for further examination. However, this dissertation sought to look beyond a focus on data protection and privacy issues to examine other problematic areas in the context of consumer protection. However, the *frame* of this dissertation allowed for a deep doctrinal analysis of only one of these problematic areas. **Section 3.1** of this chapter outlines which of the remaining problematic areas would constitute high priorities for further investigation.

2.1.3 Legal problems arising from digital consumer manipulation

One significant challenge for consumers loomed large in undertaking this enquiry. As eObjects have developed and become more prevalent over the last few years, so has the potential for unfair marketing practices that target vulnerable consumers or even create new vulnerabilities. After analysis of the existing laws regulating consumer contracts in **Chapter 6**, this dissertation concluded that substantial regulatory disconnection[1099] exists between those legal rules and the likelihood of harm brought about by the new things, conduct and relationships brought about by eObjects.

A common concern around new technologies is that the law cannot 'keep up': that is, where new technology is developed, this creates gaps in the law. This enquiry uncovered inadequacies in the law in respect of digital consumer manipulation. However, the first of these, uncertainty, is **not** a 'new' legal problem brought about by an emerging technology. Examining the current law in the context of the new things, conduct and relationships enabled by eObjects merely exposed an 'old' problem with the unconscionability principles currently used in the context of supply of goods and services to consumers. This dissertation argues that the unconscionability principles are so uncertain that they are not fit to deal

[1099] Brownsword, *Rights, Regulation, and the Technological Revolution* (n 39) ch 6. See discussion in **section 2.2.1.2** of **Chapter 3**.

with any form of significant change in business conduct or relationships, whether arising out of technological developments or from another source. This dissertation also argued that the negative effects of uncertainty are exacerbated in the context of rapid and increasingly complex sociotechnical change, and this has an effect on regulatory timing.

However, the second legal problem identified is more closely related to the specific sociotechnical change arising out of eObjects. Corporate secrecy practices and a consequential lack of transparency are long-entrenched commercial behaviours. However, these are now combined with new and powerful ways to collect, analyse, use and disseminate data for benefits that accrue overwhelmingly to business rather than the consumer. Particular attributes and interactions of eObjects are fundamental to that power, because of both the nature of the data that can be collected, and the ways in which it can be used to manipulate consumer behaviour.

2.1.4 Kickstarting reconnection

The uncovering of legal problems is a major step in establishing regulatory disconnection in the face of sociotechnical change. The logical next step is to 'reconnect' the law with the new things, activities and relationships brought about by new technologies. In this dissertation, this next step consisted of laying the groundwork for such reconnection, by proposing in broad terms the basic principles and features need in any attempt to move the existing law closer to achieving the relevant **Consumer Goals**.

When attempting reconnection of law to sociotechnical change, some of the 'usual' approaches to law reform may not be effective. The analysis in this dissertation pointed out deficiencies in both technologically specific and technologically neutral approaches. In the case of digital consumer manipulation, some of the traditional methods of consumer protection, such as disclosure and consent, have also proven ineffective in adequately protecting consumer expectations in the face of sociotechnical change.

To tackle these problems, this dissertation proposed a principle of technological appropriateness, and the combination of a general and a

specific approach to law reform. However, this approach needs also to be combined with mechanisms for swifter responses to change, such as the use of rule-making capabilities by regulators or other specialist agencies, the encouragement and funding of horizon-scanning projects and the use of more suitable consumer redress measures.

Experience in attempts at reform in the context of conventional online commerce have indicated that the pressure imposed by 'vested interests' as highlighted in the Collingridge dilemma is an ongoing problem. Therefore, urgent responses are needed, at least in relation to vulnerable and disadvantaged groups. The *frame* of this dissertation has precluded anything more than a high-level analysis of some law reform options. Therefore, further work in this area is recommended.

2.2 'Reflecting back': lessons for law and technology scholarship

2.2.1 Problems which are not 'new'

The approach taken in this dissertation was structured to mitigate the 'tendency, especially in the early years of a particular technology, to think that existing law is completely inappropriate in the new context'.[1100] The approach required a discussion of the detail of actual change brought about by emerging technological developments and the identification of specific laws that could prima facie apply to that change. However, steps were also taken to deal with arguments of scholars with the opposite tendency, who argue that problems arising out of sociotechnical change are 'overstated and … new problems can be resolved in existing frameworks'.[1101] These steps

[1100] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 283.

[1101] Ibid 284. See also Richard A Epstein, 'The Static Conception of the Common Law' (1980) 9 The Journal of Legal Studies 253, 254 ('Social circumstances continually change, but it is wrong to suppose that the substantive principles of the legal system should change in response to new social conditions'); Monroe E Price, 'The Newness of New Technology' (2001) 22 Cardozo Law Review 1885, 1896 ('It is much less the case that technological change eliminates either the need for law or reduces the capacity for establishing and enforcing norms to nothingness').

included mapping the goals of the identified pre-existing law against specific challenges with detrimental outcomes that could conflict with those goals. Additionally, the in-depth doctrinal analysis of digital consumer manipulation required the classification of legal problems into specific categories. This rigorous approach assists in avoiding both over- or under-reacting to sociotechnical change.

The results of this dissertation support the contention that the examination of the law in the context of sociotechnical change can expose 'old' legal problems anew, that is, problems that existed before the sociotechnical change at issue.[1102] It can also uncover the *exacerbation* of 'old' legal problems. This might happen in circumstances where the social conditions were such as to provoke regulatory disconnection some time before the sociotechnical change at issue. Alternatively, the problems may have always existed, such as the case where one or more of the goals or purposes of the relevant law were never achieved by the actual legal rules put in place. However, there are other difficulties that may arise in the context of reactions by lawmakers to sociotechnical change. For example, judges or legislatures may use sociotechnical change as the ostensible reason to make changes to legal rules, when in reality it is merely an excuse to change a law that the lawmaker is unhappy with for reasons other than the sociotechnical change being invoked.[1103] Therefore, it is important to differentiate between legal problems that were the result of the sociotechnical change provoking the examination, and those that are not. This differentiation allows for the proper assessment of justifications put forward for any type of law reform.[1104]

[1102] Jennifer Geetter, 'Coding for Change: The Power of the Human Genome to Transform the American Health Insurance System' (2002) 28 American Journal of Law & Medicine 1, 3; Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 284.

[1103] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 284; Epstein, 'The Static Conception of the Common Law' (n 1101) 256–65.

[1104] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 284.

However, this does not mean that in all cases a change to laws based on an 'old' problem is not justified. Very few laws exist that do not contain some defects, whether minor or major. The field of legal scholarship would be much smaller if this were not so. In **Chapter 6,** the effect of a subset of sociotechnical change brought about by the advent of eObjects was examined in-depth. When digital consumer manipulation enhanced by eObjects was examined in the light of the ACL provisions dealing with unconscionability, one of the legal problems uncovered was not a 'new' problem, but an 'old' one. The problems brought about by the uncertainty of the unconscionability provisions discussed in **Chapter 6** applies to a far wider range of conduct than that of digital consumer manipulation. Both the history of the difficulty of application of the unconscionable conduct provisions, and the difficulty in applying them to a particular subset of sociotechnical change, point to a lack of regulatory connection. This is not a case of regulatory disconnection brought about by sociotechnical change, but a case where there may never have been an appropriate connection, due to the lack of a practically useful definition of unconscionability.

This rediscovery of 'old' problems may cause frustration for scholars, but it also provides additional and valuable opportunities to revisit existing legal rules[1105] and grasp previously missed opportunities for regulatory reconnection, or an effective first-time connection. The growth in the scale of harm when 'old' legal problems are exacerbated by sociotechnical change may also justify a change in rules, particular in remedies aimed at deterring particular conduct. However, caution must be exercised in law reform, so that reconnection is achieved for the whole range of conduct and relationships that are disconnected from current rules. The reconnection should not be limited to the effects of the sociotechnical change at issue, but for the whole range of conduct left orphaned by, or mismatched with, the current regulatory regime, including 'old' conduct.

[1105] Geetter, 'Coding for Change: The Power of the Human Genome to Transform the American Health Insurance System' (n 1102) 3.

2.2.2 The nature of uncertainty

The in-depth study in **Chapter 6** was undertaken in order to discover what, if any, legal problems arose out of a distinct area of sociotechnical change, that of digital consumer manipulation enabled by eObjects. This in-depth study also provided an opportunity to clarify the general categories of legal problems that can arise in the context of sociotechnical change. Bennett Moses proposed a broad category of 'uncertainty', but confined it to a concept of 'legal' uncertainty. Excluded from the 'legal' uncertainty definition are 'uncertainties involved in litigation'. These are specified as including uncertainty in 'establishing what took place (especially if witness accounts differ)', and possibilities that the case will settle or the plaintiff withdraw.[1106] *These* exclusions (as opposed to the one discussed below relating to real ambiguities) are not contested in this dissertation, as uncertainty surrounding these issues will not have a 'legal' effect. That is, they will not have an effect on the creation or interpretation of legal rules in a judgment. Instead, settlement or withdrawal means that no judgment will exist. Uncertainty in regard to establishing facts usually creates a problem only in regard to that particular case and is unlikely to have a precedent-setting effect on *substantive* rules. Nevertheless, depending on the nature of the uncertainty, it may have an effect on litigation-specific rules, such as interpretations of rules of evidence and other 'procedural' provisions. This is not to say that these procedural rules may not have important effects. For example, a (hypothetical) procedural rule that holds that the result generated by a machine learning algorithm that cannot provide humanly-understandable explanations[1107] constitutes good – or bad – evidence would be highly significant. However, a discussion of procedural rules is beyond the scope of this dissertation.

[1106] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 250.

[1107] Edwards and Veale, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking for' (n 704) 25.

The real need for clarification arises out of Bennett Moses' additional exclusion from the uncertainty category of the 'difficulty of applying the law to the facts'.[1108] There are two types of 'difficulty' here which are discussed below, the first relating to forms of 'practical uncertainty', and the second arising out of a 'real ambiguity'. The first difficulty does not give rise to legal problems, while the second certainly does. In the first type, the difficulty arises from personal characteristics or the individual circumstances of the judge, such as intoxication, illiteracy or poor training. The most likely problem inherent in the Australian legal process arises in the context of poor training of judicial officers in relation to their understanding of particular technologies and the change they can enable. However, this is not really a *legal* problem arising out of sociotechnical change. Rather, it is a *practical* problem concerning recruitment and management of individual judicial officers. Bennett Moses argues that legal uncertainty does not exist where there is general consensus on the 'true' meaning of the law by 'reasonable members' of the legal community,[1109] even if a contrary judgment is handed down by a 'bad' judge. Presumably, sober, literate, trained and legally conformist judges will distinguish or overturn a 'legally bad' decision as soon as provided with the opportunity.

However, in relation to the second type, a difficulty in applying the law to the facts might well arise other than from a judge's idiosyncrasies or personal circumstances. Rather, it may arise from a real ambiguity arising from how the words of the rule or rules apply to new conduct, things or relationships. This is not a problem with the process of litigation or the idiosyncrasies of a particular judge, but rather a problem with the rule itself. This type of difficulty is not confined to legal problems arising out of sociotechnical change, but indeed any type of social change.

[1108] Bennett Moses, 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (n 18) 250.

[1109] Ibid 251.

It is arguable that this second type of difficulty squarely falls within the category of uncertainty. In particular, it meets the part of the definition that talks about 'where an existing category becomes ambiguous in light of new forms of conduct'.[1110] This is a serious problem in the context of sociotechnical change arising out of eObjects. For example, it may be clear that the law of negligence applies to the manufacture of an eObject, but what may be unclear is what type of design flaws would constitute negligent manufacture.

Chapter 6 outlined the problems with uncertainty around the application of the unconscionable conduct regime to digital consumer manipulation enhanced by eObjects. The analysis illustrates a problem with uncertainty arising from ambiguities which in turn arises from how the wording of legal rules applies to new conduct, things or relationships. A difficulty of applying law to the facts means that prima facie 'uncertain' legal rules may only have an *ex post* effect on conduct, once a judgment or judgments are handed down. They cannot act efficiently as *ex ante* guides to conduct. Accordingly, businesses will find it difficult to comply with 'technologically neutral' law in the face of sociotechnical change in cases where it is unclear how their conduct will be construed by a judge.

The category of uncertainty is generally important in the context of sociotechnical change. However, it is not confined to issues brought about by sociotechnical change.[1111] A particular problem in the context of sociotechnical change is that uncertainty may persist for some time, even if eventually a judge makes a clear decision. And while uncertainty continues to exist or is compounded by ambiguous and/or narrowly focussed judicial decisions, so does the potential for a surge in litigation, an increase in insurance premiums and/or insurance exclusions. All of these risks may well limit investment in and development of beneficial technologies. Additionally, this type of uncertainty may act as a brake on litigation intended to protect consumers. Limits on funding to regulators severely

[1110] Ibid 269.

[1111] Ibid 252.

restricts incentives to proactively run cases with uncertain outcomes. Furthermore, civil litigation is beyond the means of most consumers, particularly as individual monetary damage for consumer devices is likely to be small (although the increasing availability of representative actions may assist to some extent). A consequent failure to run test cases may mean the prolongation of uncertainty, and the embedding of undesirable outcomes as 'normal business practice' (as discussed in **section 4** of **Chapter 6**).

For all of the reasons outlined above, the 'real ambiguity' type of uncertainty should be clearly integrated into Bennett Moses' uncertainty category of legal problems arising out of sociotechnical change.

3 BUILDING ON THE ENQUIRY

In addition to the need for a more substantial analysis of law reform options as set out in **section 2.1.4** of this chapter, there are four key additional areas where further work building on the dissertation findings would be beneficial.

3.1 Doctrinal analysis of the remaining challenges

The level of abstraction of the *technology type* chosen for the scope of this enquiry was broad (as discussed in **section 2** of **Chapter 2**). This choice brought with it both benefits and limitations. A high-level view of the technology allowed for the extraction of technical and functional attributes and interactions that could be applied across a wide range of research agendas. It also allowed for the investigation and discovery of a broad range of challenges for consumers in **Chapter 5** of this dissertation.

However, the *frame* of this dissertation (as discussed in **section 2.1.4** of **Chapter 3**) meant that it was practical to investigate in detail legal problems for only one of the challenges faced by consumers brought about by eObjects, that of digital consumer manipulation enhanced by eObjects. Outside of this frame, the approach employed in **Chapter 6** relating to digital consumer manipulation could easily be used to analyse potential regulatory disconnection in relation to the other challenges identified in **Chapter 5**.

The goals of consumer protection laws in Australia are set out in **Chapter 3**. **Chapter 5** identified a broad range of challenges for consumers whose outcomes conflict with those goals. The challenges that were *not* subject to the in-depth analysis in **Chapter 6** now provide a research agenda for further investigation. Considering the extent of regulatory disconnection exposed in **Chapter 6** in relation to digital consumer manipulation, it is likely that further doctrinal analysis in Australia of the laws relevant to the *other* challenges in **Chapter 5** will uncover legal problems in more than one area. This is therefore a fertile area for further work.[1112]

In particular, Australian laws concerning safety and quality need urgent examination to deal with widespread security problems already evident in eObjects, and particularly the potential for physical harm.[1113] Additionally, incentives for suppliers to provide intelligible and timely information to consumers must also be evaluated to ensure that complexity of the technology does not effectively negate consumer choice and effective competition. Norms of contract law, particularly around formation of contract and chains of liability, should be examined in the context of the mechanisms of acceptance of contractual terms, and the complexity of the contractual arrangements, that are associated with eObjects and related systems. It is also important that consumer access to appropriate redress for breaches of other consumer protection principles be assured, as this forms the foundation of the efficacy of the substantive consumer protection principles. It is also important to consider whether existing product liability rules relating to causation and proof are appropriate considering the effect of

[1112] As discussed in this dissertation, some scholarly doctrinal analysis has been undertaken in jurisdictions other than Australia. For example Elvy in the US - Elvy, 'Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond' (n 94), Helberger and Wendehorst in the EU - Helberger, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' (n 42); Wendehorst, 'Consumer Contracts and the Internet of Things' (n 93).

[1113] An examination of Australian law in this area may be assisted by review of two very recent EU Directives: Directive (EU) 2019/771 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the sale of goods [2019] OJ L136/28 and Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1.

emergent properties of decision-making algorithms in eObjects (see discussion in **section 3** of **Chapter 3**).

Many of the challenges for consumers identified in **Chapter 5** were not 'new', but rather exacerbations or merely examples of challenges pre-dating eObjects. However, this does not mean that legal problems do not exist in relation to those challenges, and subsequently that they are not worthy of further investigation and analysis. As discussed in **section 2.2.1** of this chapter, an investigation of sociotechnical change can uncover instances of regulatory disconnection that existed prior to the sociotechnical change at issue.

Outside of the challenges for consumers set out in **Chapter 5**, the conceptual approach set out in **Chapter 3** is likely to be useful for detailed investigation of legal problems in other fields of enquiry, such as the investigation of the industrial Internet of Things, or challenges for corporate or government entities.

3.2 Re-including the exclusions: financial services

The doctrinal analysis of digital consumer manipulation in **Chapter 6** was limited by the exclusion from scope of laws relating to financial advice and related transactions.

During the last few years, problems with the regulation of financial advice received great scrutiny in Australia, and this scrutiny appears likely to continue for some years. This is particularly due to the publicity given to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, established on 14 December 2017, and presided over by former High Court Justice, Kenneth Hayne ('**Banking Royal Commission**').

A rich opportunity for further research exists in the area of financial advice and related transactions where these are mediated through eObjects. For example, consider an alternative version of **Vignette J14**, where the contract offered by Max and concluded by Jessica is for home insurance rather than

telecommunications services. Such a contract is likely to be subject to laws regulating general insurance under the Insurance Contracts Act 1984 (Cth) and the provision of financial advice under the Corporations Act 2001 (Cth).

The practical logistics of regulatory compliance will present significant challenges for Australian financial services licensees (AFSLs) that wish to expand the reach of their marketing and transacting activities. The presentation and timing of disclosures are likely to present challenges for both consumers and suppliers, particularly as many eObject-based transactions are able to be concluded outside of a text-based display. Analogous obligations around suitability and disclosure may apply in other areas, for example credit arrangements.[1114]

It is possible that legal problems may arise from regulatory disconnection in this specialist area. However, considering that there has been substantial legislative activity regulating the financial services industry (over and above the ACL) in the past, the existence of legal problems should not be *presumed*, as discussed in **section 3** of **Chapter 3**. It is possible that historically greater regulatory scrutiny in these areas *may* mean that the current specialist laws are better suited than the ACL to deal with detrimental outcomes for consumers as a result of eObjects. Considering the example above, it is significant that AFSLs who sell insurance are required, amongst other obligations, to assess the *appropriateness* of the insurance offered based on the best interests of their clients.[1115] This is likely to have some impact on attempts at digital consumer manipulation in the context of insurance contracts.

Further research into the possibilities of regulatory disconnection in laws regulating financial services and financial advice would be worthwhile. Such research would be opportune at the present time, as due to the outcomes of

[1114] See for example, National Consumer Credit Protection Act 2009 (Cth) sch 1 (National Credit Code).

[1115] See in particular, Corporations Act 2001 (Cth) pts 7.7, 7.7A; Australian Securities and Investments Commission, *Regulatory Guide 121: Doing Financial Services Business in Australia*.

the Banking Royal Commission, policymakers and parliamentarians are likely to feel compelled, by personal disapprobation and/or public outcry, to be in a 'reforming mood'. It is to be hoped that this reforming mood will not only extend to remediating the problems of the past, but also to meaningful consideration of the ethical and appropriate use of emerging technologies in the banking and financial services industry.

3.3 Further exploration of eObjects

In **section 2.1** of **Chapter 5**, this dissertation described an eObjects ecosystem, using the example of Noto La Diega and Walden's mapping of the Nest smart thermostat system. This mapping provided valuable insights into the complexity of contractual arrangements applicable to eObjects. Elvy's work on Contract Distancing (discussed at **section 3.5.1.2** of **Chapter 5**) also provided some insights into the problems arising from lack of proximity between consumers and contract terms, a situation obviously exacerbated when the contract terms relevant to the purchase are multiplied across many documents and parties.

Noto La Diega and Walden's map, while useful, was limited just to the Nest system. Further investigation of other eObjects ecosystems could be used to develop a general indicative network model of (at least) common interactions among Providers (defined in **section 2.1** of **Chapter 5**) in complex eObject ecosystems. Such a network model could be useful in a number of contexts. For example, it could be valuable for technical researchers tracking potential interoperability and data sharing issues, or strategic business researchers investigating useful business models. In legal research, particularly that relating to consumer protection, the model could assist in a proper investigation of the adequacy of contractual terms surrounding an eObject ecosystem. It could assist particularly in relation to issues arising out of Contract Distancing (defined in **section 3.5.1.2** of **Chapter 5**), chains of liability, and the proper alignment of the consumer protection regime against the appropriate parties to incentivise good business behaviour and allow proper redress for consumers where good behaviour is not forthcoming.

3.4 The Vignettes: good, better, best?

Chapter 4 outlined a series of Vignettes illustrating the use of eObjects and related systems in everyday life. The development of the Vignettes was based on the attributes and interactions technical research framework developed in **Chapter 2**. The use of the Vignettes enabled a useful understanding of how the attributes and interactions appear in real-life technologies, behaviours and relationships.

However, for some types of major policy development and wholesale law reform, the scope of these Vignettes would likely be insufficient. This is particularly the case when the horizontal and vertical complexity of digital markets needs to be reflected in the analysis. In order to place policy- and lawmakers in the right position to address the Collingridge dilemma, and to regulate an appropriate way at an appropriate time, some form of speculation, based on sound principles, may be more helpful. Sarewitz advocates that solely *reacting* to problems arising from the new things, activities and relationships brought about by sociotechnical change is unsatisfactory. Technological advance is not a phenomenon external to society, but one created by human choices and therefore one over which humans have control and for which they are responsible.[1116] Humans have a chance to affect the coming into being, the structure, and the behaviour of those new things, activities and relationships. However, the operation of the Collingridge dilemma would dictate that if society reacts too late, options to choose the best future paths will be limited.[1117] Speculation can play a useful part in ensuring law and policy debates are *reflexive*, rather than merely *reactive*, in particular 'stimulating discussions about what types of futures are *possible*, and what types are *desirable*'.[1118]

[1116] Daniel Sarewitz, 'Anticipatory Governance of Emerging Technologies' in Marchant, Allenby and Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (n 18).

[1117] Ibid.

[1118] Ibid 101 (emphasis added).

This limitation could be addressed in further research, by the use of the scenario studies approach, where hypothetical scenarios are developed in collaboration between multidisciplinary expert teams, as discussed in **section 2** of **Chapter 4**. The strength of this technique lies in its use of speculation that is not unbounded or untested, but is derived from the work of groups of experts in different disciplines and/or professions. This approach, while too resource-intensive to be encompassed within a single doctoral study, is nevertheless a robust one for policy development and the identification of legal problems in important areas.

Such an approach could contribute to a vigorous investigation of not just current, but also sociotechnical change that appears or is widely proclaimed to be, imminent, and perhaps also radical. The use of a panel of inter- and multi-disciplinary experts means that this investigation could be founded not just on technical disciplines, but also on other areas such as philosophy, ethics and regulatory theory. Studies of implications of sociotechnical change that consider issues outside the technology itself are sorely needed in early-stage studies of rapidly developing technology.

For example, society as a whole is only just starting to 'catch up' with the implications of wholesale collection, use and misuse of large amounts of data by corporate actors. Existing legal frameworks are such that they protect the confidentiality of corporate actors' data businesses, while at the same time private information about individuals' lives, hopes and fears is seen as a commodity to be taken without real permission or recompense and then traded to every organisation willing to pay. There is a massive amount of consumer data already 'in the wild', due to conventional ecommerce practices,[1119] and data collection by existing eObjects continues apace. Realistically, much of this data cannot be 'returned' to consumers. It has escaped for good. The sheer volume of data that has already been extracted, particularly when it cannot be attributed to a particular person but may

[1119] Christl, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (n 649).

nevertheless be employed against them, may mean that regulation now may be too late to avoid some of the harms created. At the very least it will be 'expensive, dramatic, and resisted'[1120] by corporate entities whose business models rely on data, as predicted by discussions on the Collingridge dilemma.

The introduction of 'privacy by design' principles, such as those now contained in Article 25 of the GDPR, may help future generations. However, even when finally implemented, 'by design' principles cannot realistically put the genie back in the bottle for those who have already been subjected to the massive levels of dataveillance enabled by widespread use of information technology and allowed to flourish by weak data protection and privacy laws (as discussed in **section 3.5.1** of **Chapter 6**). A strong consumer protection approach, which targets inappropriate use of data already collected, *may* be able to overcome some of these existing problems. However, if policymakers had been able to pay greater attention to implications such as these at an earlier stage, some of the harms may have been prevented, and the practices that give rise to them may not have become widespread.

If the implications of sociotechnical change can be better anticipated, they can be better prepared for by policymakers and regulators.[1121] Accurate predictions of future sociotechnical change are undeniably difficult to make, and the ruminations of a single researcher on a purely speculative technology is limited as an agenda for useful policy research. However, a consensus expectation developed by a reasonably-sized team of interdisciplinary experts is more likely to be important, and (hopefully) much less likely to be written off as mere 'doomsaying'[1122], entrenched techno-pessimism or self-interested promotion. Also, there is much more

[1120] Goodwin, 'Introduction: A Dimensions Approach to Technology Regulation' (n 393) 2.

[1121] See also Brownsword, *Rights, Regulation, and the Technological Revolution* (n 18) 284.

[1122] Such as that derided in Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (n 488) 29.

hope that policymakers and regulators will consider the issues in time to meaningfully grapple with them before jurisdictions end up on the wrong side of a regulatory timing problem. This hope is dependent on the results of these scenario studies being embedded in the policy making and regulatory process, such as in a 'technology assessment panel' model.[1123]

4 FINAL REMARKS

In 1991, Weiser's view of the future of eObjects was somewhat utopian: 'machines that fit the human environment, instead of forcing humans to enter theirs, will make using a computer as refreshing as taking a walk in the woods.'[1124] His vision of the 'third wave' of computing has been partially achieved, but in a somewhat different form than he and other early visionaries anticipated. eObjects and the systems in which they participate have enabled significant sociotechnical change, with a wide range of new devices, conduct and relationships emerging. The relevant technologies are still developing, and may still take divergent paths. However, the current dominant mode is less on the 'refreshing' side, and closer to Dourish and Bell's 'messy' and 'heterogenous' description.[1125]

Surfing the third wave of computing may be exhilarating for many, but it is not a safe ride. Surfboards can break, rocks and sharks abound, and the next wipe-out is just around the corner. In navigating the world of eObjects, consumers must deal with 'buggy and brittle' technologies, a loss of control and choice, and exploitative conduct by suppliers and other corporate interests. They must deal with the introduction of new complexities, not only in the technologies themselves, but in the legal and social arrangements surrounding their use. The potential for disconnection between these

[1123] For a detailed history and literature review of public technology assessment initiatives and panels, see Bennett Moses, 'Agents of Change: How the Law Copes with Technological Change' (n 140) 774–79.

[1124] Weiser, 'The Computer for the 21st Century' (n 19) 104.

[1125] Dourish and Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (n 159) 25.

challenges and current legal regimes adds to these problems: in many places there may be no flags to swim between, and no surf lifesavers on duty.

This dissertation aimed to contribute to flagging the danger areas for consumers, and to make a call for thoughtful engagement by policymakers, judges and legislators with the challenges posed by eObjects and the systems in which they participate. Initial ignorance of the effects of the third wave is now giving way to a body of consumers who are both fearful and disempowered. Time and again over the course of doctoral study the author of this dissertation has seen consumer reaction to sociotechnical change as one of 'Hobson's choice'. Consumers feel that they must accept a technology with all of its attendant problems, or refuse to use it at all. Taken to extremes, this may lead to a denial of the great potential of some of these technologies to actually make life significantly better: for example, in assisting those with disabilities, in healthcare, in aged care, in efficient infrastructure, transport, industry and agriculture.

The history of consumer protection law has been a continuing war against the dangers of a 'caveat emptor' approach. When consumer protection battles have been won, the resulting safety net for consumers has actually encouraged the development of new products and industries. In the past, society has been able to reach some form of consensus on what types of corporate conduct are unacceptable, and legislate accordingly. The use and abuse of eObjects and the systems in which they participate may currently fit only awkwardly within our current consumer protection regime, but there is no reason why this fit cannot be made better. The 'change' in sociotechnical change is also a crucial consideration: one-off solutions will likely be insufficient to deal with the continuing evolution of these technologies, so effective mechanisms for continuing evolution in law and policy must also be put in place. These mechanisms should include pro-active and swiftly reactive policy and rule-making bodies and processes, the use of appropriate language and interpretative principles in legislation and judicial decision-making, and well-resourced, informed and activist regulators.

Appendix A

Table 8: Poslad's properties and sub-properties[1126]

Core properties	Sub-properties
Distributed	universal, seamless, heterogeneous networked synchronised, coordinated open transparent, virtual mobile, nomadic
iHCI	non-intrusive, hidden, invisible, calm computing tangible, natural anticipatory, speculative, pro-active affective, emotive user-aware post-human sense of presence, immersed, virtual, mediated reality
Context-aware	sentient, unique, localised, situated adaptive, active context-aware person-aware, user-aware, personalised, tailored environment-aware, context-aware, physical context-aware ICT awareness
Autonomous	automatic embedded, encapsulated, embodied resource-constrained untethered, amorphous autonomic, self-managing, self-star emergent, self-organising

[1126] **Table 8** is a consolidation of Tables 1.1–1.5 in Poslad, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (n 192) 19.

Core properties	Sub-properties
Intelligent	reactive, reflex model-based, rules/policy-based logic/reasoning goal-oriented, planned, pro-active utility-based, games theoretic learning, adaptive co-operative, collaborative, benevolence competitive, self-interested, antagonistic, adversarial orchestrator, choreographed, mediated task-sharing communal, shared meaning shared knowledge speech-act based, intentional, mentalistic emergent

Bibliography

Aarts E and Roovers R, 'IC Design Challenges for Ambient Intelligence' *Proceedings of the Design, Automation, and Test in Europe Conference and Exhibition 2003* (IEEE Computer Society 2003) 2

Aarts EHL and Encarnação JL (eds), *True Visions: The Emergence of Ambient Intelligence* (Springer-Verlag 2006)

Ablon L, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data* (Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, 15 March 2018)

Access Canberra (Australian Capital Territory) and others, 'Compliance and Enforcement: How Regulators Enforce the Australian Consumer Law' (January 2017) <https://cdn.tspace.gov.au/uploads/sites/86/2019/01/ACL_Compliance_and_enforcement_guide.pdf> accessed 30 June 2017

Acquity Group, 'The Internet of Things: The Future of Consumer Adoption' (2014) <https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf> accessed 30 June 2018

Adams D, *The Salmon of Doubt: Hitchhiking the Galaxy One Last Time* (Harmony Books 2002)

Adelstein F and others, *Fundamentals of Mobile and Pervasive Computing* (McGraw-Hill 2005)

Agency for Science Technology and Research Singapore, 'Smart Interactive Billboard Device' (US Patent Application US20050021393A1) <https://patents.google.com/patent/US20050021393A1/en> accessed 5 September 2018

Akerlof GA, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 Quarterly Journal of Economics 488

Alaba FA and others, 'Internet of Things Security: A Survey' (2017) 88 Journal of Network and Computer Applications 10

Alizadeh T, Helderop E, and Gubresic T, 'Around 50% of homes in Sydney, Melbourne and Brisbane have the oldest NBN technology' (*The Conversation*, 7 May 2019) <https://theconversation.com/around-50-

of-homes-in-sydney-melbourne-and-brisbane-have-the-oldest-nbn-technology-115131> accessed 10 May 2019

Amazon, 'Amazon Dash Replenishment Terms of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=201730770> accessed 12 July 2018

—— 'Amazon Dash Terms of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=202002080> accessed 11 July 2018

—— 'Amazon Prime Air' <www.amazon.com/Amazon-Prime-Air/b?node=8037720011> accessed 25 August 2018

—— 'Amazon.com Privacy Notice' (29 August 2017) <www.amazon.com/gp/help/customer/display.html?nodeId=468496> accessed 11 July 2018

—— 'Conditions of Use' <www.amazon.com/gp/help/customer/display.html?nodeId=201909000> accessed 11 July 2018

—— 'Echo and Alexa' <www.amazon.com/all-new-amazon-echo-speaker-with-wifi-alexa-dark-charcoal/dp/B06XCM9LJ4/ref=sr_1_cc_1?s=aps&ie=UTF8&qid=1534996023&sr=1-1-catcorr&keywords=echo+speaker+alexa> accessed 23 August 2018

—— 'Tide Dash Button: Save 5% on All Products Ordered through This Button' <www.amazon.com/Tide-Dash-Button-products-ordered/dp/B0187TMRYM/ref=sr_1_1?ie=UTF8&qid=1531363704&sr=8-1&keywords=amazon+dash+button> accessed 11 July 2018

American Bar Association Section of Science & Technology Law, Submission to the National Telecommunications and Information Administration, US Dept of Commerce, in response to Docket No. 160331306-6306-01: The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things (2016)

American Law Institute, The, and National Conference of Commissioners on Uniform State Laws, *Uniform Commercial Code* (2017-2018 edn, Thomson Reuters 2017)

Analog Devices, 'SmartMesh WirelessHART' <www.linear.com/products/smartmesh_wirelesshart> accessed 9 September 2018

Andreou A and others, 'Investigating Ad Transparency Mechanisms in Social Media: A Case Study of Facebook's Explanations' (Network and

Distributed Systems Security (NDSS) Symposium 2018, San Diego, February 2018)

ANEC and others, *Securing Consumer Trust in the Internet of Things: Principles and Recommendations 2017* (November 2017)

Angwin J and others, 'Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased Against Blacks' (*ProPublica*, 23 May 2016) <www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 1 May 2018

Antonenko PD, 'The Instrumental Value of Conceptual Frameworks in Educational Technology Research' (2015) 63 Educational Technology Research and Development 53

Apple, 'Choose the Apple Watch That's Right for You' <www.apple.com/au/shop/buy-watch/apple-watch> accessed 9 September 2018

Arnold DN, 'The Patriot Missile Failure' (23 August 2000) <www-users.math.umn.edu/~arnold/disasters/patriot.html> accessed 7 July 2018

Arthur WB, 'Competing Technologies, Increasing Returns, and Lock-In by Historical Events' (1989) 99 The Economic Journal 116

Ashton K, 'That "Internet of Things" Thing' (*RFID Journal*, 22 June 2009) <www.rfidjournal.com/articles/view?4986> accessed 26 February 2015

Association for Computing Machinery, 'UbiComp 2013' <www.ubicomp.org/ubicomp2013/index.php> accessed 20 June 2018

August, 'Smart Lock Pro + Connect' <https://store.august.com/products/august-smart-lock-pro-connect?utm_source=5056&utm_medium=DIS&utm_campaign=a22-a325-a4020-07> accessed 24 August 2018

Australia, Attorney-General's Department, *Improving Australia's Law and Justice Framework* (Discussion Paper, 2012)

Australia, Commonwealth Government Response to the Senate Standing Committee on Economics Report on 'The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974' (November 2009)

Australia, Department of Industry Innovation and Science, 'Smart Grid, Smart City' <http://webarchive.nla.gov.au/gov/20160615043539/http://www.industry.gov.au/Energy/Programmes/SmartGridSmartCity/Pages/default.aspx> accessed 9 September 2018

Australia, Department of Infrastructure, Regional Development and Cities, 'Smart Cities and Suburbs', <https://infrastructure.gov.au/cities/smart-cities/> accessed 23 August 2018

Australia, Department of Prime Minister and Cabinet, *The Australian Government Guide to Regulation* (March 2014)

—— *The Australian Government's Response to the Productivity Commission Data Availability and Use Inquiry* (1 May 2018) <www.pc.gov.au/inquiries/completed/data-access/data-availability-use-government-response.pdf> accessed 28 May 2018

Australia, 'Issues Paper Submissions' (*Competition Policy Review*, 2014) <http://competitionpolicyreview.gov.au/issues-paper/submissions/> accessed 1 November 2017

Australia, Senate Standing Committee on Economics, 'The Need, Scope and Content of a Definition of Unconscionable Conduct for the Purposes of Part IVA of the Trade Practices Act 1974' (December 2008)

Australia, Treasury, *The Nature and Application of Unconscionable Conduct Regulation: Can Statutory Unconscionable Conduct be Further Clarified in Practice?* (Issues Paper, November 2009)

—— 'Consumer Voices: Sustaining Advocacy and Research in Australia's New Consumer Policy Framework', <http://archive.treasury.gov.au/contentitem.asp?ContentID=1532>, accessed 10 September 2019

Australian Communications and Media Authority, *Optimal Conditions for Effective Self- and Co-regulatory Arrangements* (Occasional Paper, June 2015)

—— *The Internet of Things and the ACMA's Areas of Focus: Emerging Issues in Media and Communications* (Occasional Paper, November 2015) <www.acma.gov.au/theACMA/~/media/18E314A0C00A41F9B4D629DAB9397436.ashx> accessed 20 June 2018

Australian Competition and Consumer Commission, *Advertising and Selling Guide* (November 2017)

—— *Business Snapshot: Unconscionable Conduct* (12 September 2012) <www.accc.gov.au/publications/business-snapshot/unconscionable-conduct> accessed 30 June 2018

—— *Digital Platforms Inquiry Final Report* (June 2019)

—— *Digital Platforms Inquiry: Preliminary Report* (December 2018)

—— *Platform Operators in the Sharing Economy: A Guide for Complying with the Competition and Consumer Law in Australia* (3 November 2016)

—— Small Claims Tribunals <https://www.accc.gov.au/contact-us/other-helpful-agencies/small-claims-tribunals> accessed 12 May 2019

Australian Council of Learned Academies, 'ACOLA Receives ARC Funding to Undertake Two New Horizon Scanning Projects on AI and IoT' (Media Release, 21 May 2018) <https://acola.org.au/wp/acola-receives-arc-funding-to-undertake-two-new-horizon-scanning-projects-on-ai-and-iot/> accessed 12 September 2019

Australian Law Reform Commission, *Copyright and the Digital Economy* (Discussion Paper 79, May 2013)

—— *For Your Information: Australian Privacy Law and Practice* (Report 108, May 2008)

Australian Legal Information Institute, 'AustLII' <www.austlii.edu.au/> accessed 30 June 2018

Australian Securities and Investments Commission, Regulatory Guide 121: Doing Financial Services Business in Australia (July 2013)

—— Submission No 1 Supplementary to Submission No 45 to Senate Standing Committee on Economics, *The Performance of the Australian Securities and Investments Commission* (October 2013) <www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/ASIC/Submissions>

Baldwin R, Cave M and Lodge M, 'Introduction: Regulation – The Field and the Developing Agenda' in Baldwin R and others (eds), *The Oxford Handbook of Regulation* (OUP 2010)

Barcena MB, Wueest C and Lau H, *How Safe is Your Quantified Self?* (Symantec Security Response Report, 11 August 2014)

Barlow JP, 'A Declaration of the Independence of Cyberspace' (1996) 56 Humanist 18

Barocas S and Selbst AD, 'Big Data's Disparate Impact' (2016) 104 California Law Review 671

Barrett B, 'After Backlash, Logitech Will Upgrade All Harmony Link Owners for Free' (*Wired*, 9 November 2017) <www.wired.com/story/logitech-giving-harmony-link-owners-a-free-harmony-hub/> accessed 11 July 2018

Barter C and Renold E, 'The Use of Vignettes in Qualitative Research' (Social Research Update 25, Summer 1999) <http://sru.soc.surrey.ac.uk/SRU25.html> accessed 25 November 2016

Basil Leaf Technologies, 'DXTER™: A New Kind of Consumer Medical Device' <www.basilleaftech.com/dxter/> accessed 31 December 2018

Baumer E, 'Usees' (Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, April 18-23 2015)

Beaconnected <https://beaconnected.com.au/> accessed 23 August 2018

Beebe B, 'Law's Empire and the Final Frontier: Legalizing the Future in the Early Corpus Juris Spatialis' (1999) 108 Yale Law Journal 1737

Behmor <https://behmor.com/> accessed 25 August 2018

Ben-Shahar O and Schneider CE, *More than You Wanted to Know: The Failure of Mandated Disclosure* (Princeton UP 2014)

Bennett Moses L, 'Adapting the Law to Technological Change: A Comparison of Common Law and Legislation (Australia)' (2003) 26 University of New South Wales Law Journal 394

—— 'Agents of Change: How the Law Copes with Technological Change' (2011) 20 Griffith Law Review 763

—— 'Exploring Technological Frontiers: Autonomy in Legal Scholarship' (2010) 30 Bulletin of Science, Technology & Society 22

—— 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target' (2013) 5 Law, Innovation and Technology 1

—— 'Recurring Dilemmas: The Law's Race to Keep Up with Technological Change' (2007) 2 University of Illinois Journal of Law, Technology & Policy 239

—— 'Regulating Beyond Nanotechnology' (2011) 30 IEEE Technology and Society Magazine 42

—— 'Regulating in the Face of Sociotechnical Change' in Brownsword R, Scotford E and Yeung K (eds), *Oxford Handbook of Law and Regulation of Technology* (OUP 2017)

—— 'Sui Generis Rules', in Marchant GE, Allenby BR and Herkert JR, Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem

—— 'Understanding Legal Responses to Technological Change: The Example of In Vitro Fertilization' (2005) 6 Minnesota Journal of Law, Science & Technology 505

—— 'Why Have a Theory of Law and Technological Change?' (2007) 8 Minnesota Journal of Law, Science & Technology 589

Bennett Moses L and Chan J, 'Algorithmic Prediction in Policing: Assumptions, Evaluation, and Accountability' (2018) Policing and Society 1

Bergh D and others, 'Information Asymmetry in Management Research: Past Accomplishments and Future Opportunities' (2019) 45 Journal of Management 122

Berlin AA and Gabriel KJ, 'Distributed MEMS: New Challenges for Computation' (1997) 4 IEEE Computational Science and Engineering 12

Bernstein G, 'The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy' (2006) 39 Connecticut Law Review 241

—— 'When New Technologies Are Still New: Windows of Opportunity for Privacy Protection' (2006) 51 Villanova Law Review 921

Best J, 'Building the Tricorder: The Race to Create a Real-Life Star Trek Medical Scanner' (*ZDNet*, 26 November 2018) <www.zdnet.com/article/building-the-tricorder-the-race-to-create-a-real-life-star-trek-medical-scanner/> accessed 31 December 2018

Bigelow P, 'Car Companies Say Home Repairs Are "Legally Problematic," Seek Copyright Restrictions' (*Autoblog*, 20 April 2015) <www.autoblog.com/2015/04/20/automakers-gearheads-car-repairs/> accessed 10 September 2018

Bijker WE, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (MIT Press 1995)

Bilton N, 'Disruptions: As New Targets for Hackers, Your Car and Your House' *The New York Times* (New York, 11 August 2013) <http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0> accessed 2 February 2017

Birks P, 'Definition and Division: A Meditation on Institutes' in Birks P (ed) *The Classification of Obligations* (OUP 1997)

Birks P and Yin CN, 'On the Nature of Undue Influence' in Beatson J and Friedmann D (eds), *Good Faith and Fault in Contract Law* (OUP 1995)

Black J, 'Critical Reflections on Regulation' (2002) 27 Australian Journal of Legal Philosophy 1

—— 'Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a "Post-Regulatory" World' (2001) 54 Current Legal Problems 103

Bloomberg News, 'Quicktake: The Great Firewall of China' *Bloomberg* (6 November 2018) <www.bloomberg.com/quicktake/great-firewall-of-china> accessed 4 March 2019

Blink, 'End User License Agreement' <https://blinkforhome.com/pages/eula?locale=en> accessed 26 April 2019

Boeckl K and others, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* (National Institute of Standards and Technology Internal Report 8228 (Draft), September 2018)

Bogle A, 'I Asked Everyone from Facebook to Data Brokers to Stan for My Information. It Got Messy' *ABC Radio Australia* (28 April 2018) <www.radioaustralia.net.au/international/2018-04-28/i-asked-everyone-from-facebook-to-data-brokers-to-stan-for-my-information-it-got-messy/1752610> accessed 28 April 2018

Bol N, Helberger N and Weert JCM, 'Differences in Mobile Health App Use: A Source of New Digital Inequalities?' (2018) 34 The Information Society 183

Bolden S, 'Personal Robots Helping Elderly in Their Homes' *Telstra iCareHealth,* (9 November 2015) <www.icarehealth.com.au/blog/personal-robots-helping-elderly-in-their-homes/> accessed 29 January 2018

Borgström S and Mauerhofer V, 'Developing Law for the Bioeconomy' (2016) 34 Journal of Energy & Natural Resources Law 373

Bosua R and others, 'Privacy in a World of the Internet of Things: A Legal and Regulatory Perspective' (2017) Networked Society Institute Research Paper 6

Boult A, Criddle C and McGoogan C, 'Apple's New iOS 10 Update Causes Major 'Bricking' Problems for iPhone and iPad Users' *The Telegraph* (London, 15 September 2016) <www.telegraph.co.uk/technology/2016/09/13/ios-10-launch-live-how-to-upgrade-to-apples-new-software-and-wha/> accessed 30 October 2016

Bowles N, 'Thermostats, Locks and Lights: Digital Tools of Domestic Abuse' *The New York Times* (New York, 23 June 2018) <www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html> accessed 25 June 2018

Braithwaite J, 'Responsive Regulation and Developing Economies' (2006) 34 World Development 884

Brenner SW, 'Law in an Era of Pervasive Technology' (2006) 15 Widener Law Journal 667

—— *Law in an Era of 'Smart' Technology* (OUP 2007)

Briden P, 'Google Glass Review: Glass in Its Current Form is Dead' (*Know Your Mobile*, 11 April 2014) <www.knowyourmobile.com/google/google-glass/21388/google-glass-release-date-features-and-price-ray-ban-oakley-commit-future> accessed 13 June 2018

Brody G and Temple K, 'Unfair but Not Illegal: Are Australia's Consumer Protection Laws Allowing Predatory Businesses to Flourish?' (2016) 41 Alternative Law Journal 169

Brookman J and others, 'Cross-Device Tracking: Measurement and Disclosures' (2017) 2 Proceedings on Privacy Enhancing Technologies 133

Browne MN and others, 'Protecting Consumers from Themselves: Consumer Law and the Vulnerable Consumer' (2014) 63 Drake Law Review 157

Brownsword R, 'Code, control, and choice: why East is East and West is West' (2005) 25 Legal Studies 1

—— *Rights, Regulation, and the Technological Revolution* (OUP 2008)

—— 'Techno-Regulation, Human Rights and Human Dignity' in Brownsword R (ed) *Human Rights* (Hart Publishing 2004)

Brownsword R and Goodwin M, Law and the Technologies of the Twenty-First Century: Text and Materials (CUP 2012)

Brownsword R, Scotford E and Yeung K, 'Law, Regulation, and Technology: The Field, Frame, and Focal Questions' in Brownsword R and others (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017)

Bruce A, *Consumer Protection Law in Australia* (2nd edn, LexisNexis Butterworths 2014)

Buchanan WJ, Li S and Asif R, *Lightweight Cryptography Methods* (Taylor & Francis 2017)

Burdon M and Harpur P, 'Re-Conceptualising Privacy and Discrimination in an Age of Talent Analytics' (2014) 37 University of New South Wales Law Journal 679

Burrell J, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) Big Data & Society 1

Burrows A, *Understanding the Law of Obligations: Essays on Contract, Tort and Restitution* (Hart Publishing 1998)

Butler S, *Macquarie Dictionary: Australia's National Dictionary Online* (Macquarie Library 2003)

Cadwalladr C and Graham-Harrison E, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (Sydney, 18 March 2018) <www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 18 March 2018

Calo R, 'Digital Market Manipulation' (2014) 82 George Washington Law Review 995

—— 'Tiny Salespeople: Mediated Transactions and the Internet of Things' (2013) 11 IEEE Security & Privacy Magazine 70

Campbell M, 'Lawsuit Seeks More than $5M from Apple for Slowing Older iPhones with iOS 9 Upgrade' (*Appleinsider*, 29 December 2015) <http://appleinsider.com/articles/15/12/29/lawsuit-seeks-more-than-5m-from-apple-for-allegedly-slowing-older-iphones-with-ios-9-upgrade> accessed 30 October 2016

Caron X and others, 'The Internet of Things (IoT) and Its Impact on Individual Privacy: An Australian Perspective' (2016) 32 Computer Law & Security Review 4

Carruthers K, 'How the Internet of Things Changes Everything: The Next Stage of the Digital Revolution' (2014) 2 Australian Journal of Telecommunications and the Digital Economy 69.1

Carter JW, *Contract Law in Australia* (6th edn, LexisNexis Butterworths 2013)

Centre for Data Ethics and Innovation (CDEI) <https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei> accessed 9 May 2019

Čerka P, Grigienė J and Sirbikytė G, 'Is It Possible to Grant Legal Personality to Artificial Intelligence Software Systems?' (2017) 33 Computer Law & Security Review 685

Cha B, 'A Beginner's Guide to Understanding the Internet of Things' (*recode*, 15 January 2015) <http://recode.net/2015/01/15/a-beginners-guide-to-understanding-the-internet-of-things/> accessed 3 May 2016

Chadwick J, 'Australian Smart Home Device Market Grew 55 Percent In 2017: Telsyte' (*ZDNet*, 26 November 2018) <www.zdnet.com/article/australian-smart-home-device-market-grew-55-percent-in-2017-telsyte/> accessed 27 August 2018

Chaouchi H (ed), *The Internet of Things: Connecting Objects to the Web* (John Wiley & Sons 2010)

Charlesworth A, 'The Ascent of Smartphone' (2009) 4 Engineering and Technology 32

Chatham House (The Royal Institute of International Affairs), 'Chatham House Rule' <www.chathamhouse.org/chatham-house-rule> accessed 9 September 2018

Checkoway S and others, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' (Proceedings of USENIX Security 2011, August 2011)

Cherry MA, 'A Eulogy for the EULA' (2014) 52 Duquesne Law Review 335

Christl W, *Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* (A Report by Cracked Labs, Vienna, June 2017)

Christl W and Spiekermann S, *Networks of Control: A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy* (facultas 2016)

Cimpanu C, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks across London' (*Softpedia*, 20 October 2015) <http://news.softpedia.com/news/insecure-internet-connected-kettles-help-researchers-crack-wifi-networks-across-london-494895.shtml> accessed 12 November 2015

Clark DS, 'Comparative Law Methods in the United States' (1998) 16 Roger Williams University Law Review 134

Clarke R, 'Cyborg Rights' (2011) 30 IEEE Technology and Society Magazine 49

—— 'Information Technology and Dataveillance' (1988) 31 Communications of the ACM 498

—— 'Instrumentalist Futurism: A Tool for Examining IT Impacts and Implications' (6 October 1997) <www.rogerclarke.com/DV/InstFut.html> accessed 24 November 2016

—— 'Origins and Nature of the Internet in Australia' (*Xamax Consultancy*, 29 January 2004) <www.rogerclarke.com/II/OzI04.html> accessed 13 May 2015

—— 'Paradise Gained, Paradise Re-Lost: How the Internet Is Being Changed from a Means of Liberation to a Tool of Authoritarianism' (2001) 18 Mots Pluriels

—— 'Quality Assurance for Security Applications of Big Data' (Proceedings of the European Intelligence and Security Informatics Conference, Uppsala, 17–19 August 2016)

—— 'Quality Factors in Big Data and Big Data Analytics' (19 December 2014) <www.rogerclarke.com/EC/BDQF.html#DQF> accessed 23 October 2018

—— 'Risks Inherent in the Digital Surveillance Economy: A Research Agenda' (2019) 34 Journal of Information Technology 1

—— 'Scenario-Based Research' (*Xamax Consultancy*, 26 June 2003) <www.xamax.com.au/Res/Scenarios.html> accessed 22 August 2018

—— 'The Effectiveness of Privacy Policy Statements' in D Kerr and others (eds), *Digital Business Security Development: Management Technologies* (IGI Global 2011)

—— 'Understanding the Drone Epidemic' (2014) 30 Computer Law and Security Review 230

—— 'What Drones Inherit from their Ancestors' (2014) 30 Computer Law & Security Review 247

Clarke R and Bennett Moses L, 'The Regulation of Civilian Drones Impacts on Public Safety' (2014) 30 Computer Law and Security Review 263

Class Action Complaint for Violations of the Electronic Communications Privacy Act 18 USC PP 2510, Satchell v Sonic Notify Inc d/b/a Signal360

Class Action Complaint, NP v Standard Innovation (US) Corp, Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois (Filed 2 September 2016)

Class Action Settlement Agreement, NP v Standard Innovation (US) Corp, Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois (Filed 9 March 2017)

Clifford D, 'Citizen-Consumers in a Personalised Galaxy: Emotion Influenced Decision-Making – A True Path to the Dark Side?' (CiTiP Working Paper 31/2017, KU Leuven Centre for IT & IP Law, submitted 15 September 2017)

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3037425> accessed 30 April 2018

Cloud Security Alliance, 'Security Guidance for Early Adopters of the Internet of Things (IoT)' (Mobile Working Group, Peer Reviewed Document, April 2015) <https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf> accessed 8 July 2017

Cockfield AJ, 'Towards a Law and Technology Theory' (2004) 30 Manitoba Law Journal 383

Cockfield AJ and Pridmore J, 'A Synthetic Theory of Law and Technology' (2007) 8 Minnesota Journal of Law, Science & Technology 475

Code Curmudgeon, 'IoT Hall-of-Shame' <https://codecurmudgeon.com/wp/iot-hall-shame/> accessed 9 July 2018

Coen R and others, 'A User-Centered Perspective on Algorithmic Personalization' (Master of Information Management and Systems: Final Project, University of California, Berkeley, 6 May 2016)

Coll L and Simpson R, *Connection and Protection in the Digital Age: The Internet of Things and Challenges for Consumer Protection* (Consumers International, April 2016)

Collingridge D, *The Social Control of Technology* (Pinter 1980)

Colombus L, 'Roundup of Internet of Things Forecasts and Market Estimates: 2018' (*Enterprise Irregulars*, 2 January 2018) <www.enterpriseirregulars.com/121867/roundup-internet-things-forecasts-market-estimates-2018/> accessed 27 August 2018

Commonwealth of Australia, *Parliamentary Debates (Second Reading Speech)* House of Representatives 14 June 2009, 6981-9 (Craig Emerson)

Comstock J, 'Medtronic Launches Smartphone Connectivity for CGMs, Insulin Pumps' (*mobihealthnews*, 29 September 2015) <www.mobihealthnews.com/47112/medtronic-launches-smartphone-connectivity-for-cgms-insulin-pumps> accessed 26 March 2018

Consumer Affairs Australia and New Zealand, *Australian Consumer Law Review: Final Report* (March 2017)

—— *Australian Consumer Law Review: Interim Report* (October 2016)

Consumer Policy Research Centre, 'Data Protection Rules Are Failing Australian Consumers' (Fact Sheet, 2018)

<https://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy/fact_sheet_-_data_protection_rules_failing_australian_consumers/> accessed 23 May 2018

Consumer Reports, 'Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds' (*Consumer Reports*, 7 February 2018) <www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/> accessed 8 August 2018

Consumers International, *Consumer Protection: Why It Matters to You: A Practical Guide to the United Nationals Guidelines for Consumer Protection* (2016)

—— 'Frequently Asked Questions: What are the Consumer Rights?' <https://www.consumersinternational.org/who-we-are/faqs/#frequently-asked-questions-what-are-the-consumer-rights> accessed 10 September 2019.

—— *Testing Our Trust: Consumers and the Internet of Things 2017 Review* (October 2017)

—— 'Who we are' <https://www.consumersinternational.org/who-we-are/our-history/> accessed 10 September 2019.

Cook DJ, Augusto JC and Jakkula VR, 'Ambient Intelligence: Technologies, Applications, and Opportunities' (2009) 5 Pervasive and Mobile Computing 277

Coote B, 'The Essence of Contract (Part II)' (1989) 1 Journal of Contract Law 183

Corero, 'Corero DDoS Trends Report Q2–Q3 2017' (2017) <http://info.corero.com/rs/258-JCF-941/images/2017-q2q3-ddos-trends-report.pdf> accessed 10 July 2018

Corkery M and Silver-Greenberg J, 'Miss a Payment? Good Luck Moving That Car' *The New York Times* (New York, 24 September 2014) <http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_php=true&_type=blogs&ref=business&_r=0> accessed 2 February 2017

Corones SG, 'Consumer Guarantees in Australia: Putting an End to the Blame Game' (2009) 9 Queensland University of Technology Law and Justice Journal 137

—— *The Australian Consumer Law* (3rd edn, Lawbook Co 2016)

Correa D, 'IoT Lightbulb Worm Takes Over All Smart Lights until Entire City Is Infected' (*SC Magazine*, 10 November 2016) <www.scmagazineuk.com/iot-lightbulb-worm-takes-smart-lights-until-entire-city-infected/article/1475933> accessed 14 December 2016

Cortez N, 'Regulating Disruptive Innovation' (2014) 29 Berkeley Technology Law Journal 175

Coulouris GF and others, *Distributed Systems: Concepts and Design* (Addison-Wesley 2012)

Council of Australian Governments, Intergovernmental Agreement for the Australian Consumer Law (2 July 2009)

Council of Australian Law Deans, *CALD Statement on the Nature of Legal Research* (May and October 2005)

Council of Europe, Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes (Adopted by the Committee of Ministers on 13 February 2019 at the 1337th meeting of the Ministers' Deputies) ((Decl(13/02/2019)1)

Coyne A, 'Starved of Funding, Resources, OAIC is Left to Shrivel' (*IT News*, 17 July 2015) <www.itnews.com.au/blogentry/starved-of-funding-resources-oaic-is-left-to-shrivel-405273> accessed 23 March 2018

Craswell R, 'Interpreting Deceptive Advertising' (1985) 65 Boston University Law Review 657

Crozier R, 'Chemist Warehouse Could Create an Internet of Medicine' (*iTnews*, 18 October 2018) <www.itnews.com.au/news/chemist-warehouse-could-create-an-internet-of-medicine-514130> accessed 18 October 2018

D'Agostino E, *Contracts of Adhesion Between Law and Economics: Rethinking the Unconscionability Doctrine* (Springer 2015)

Dannecker K and others, 'A Comparison of Energy Expenditure Estimation of Several Physical Activity Monitors' (2013) 45 Medicine and Science in Sports and Exercise 2105

Das R and others, 'Security Based Domotics' (2013) 10 Procedia Technology 942

Dastin J, 'Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women' (*Reuters*, 10 October 2018) <www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G> accessed 23 October 2018

Davidson D, 'Facebook Exploits 'Insecure' To Sell Ads' *The Australian* (Sydney, 1 May 2017) <www.theaustralian.com.au/business/media/digital/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6> accessed 21 May 2018

Davies A, 'The Wired Guide to Self-Driving Cars' (*Wired*, 1 February 2018) <www.wired.com/story/guide-self-driving-cars/> accessed 23 August 2018

De Hert P and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law & Security Review 193

Dias-Abey M, 'Balancing Employee Protection with Promoting Business Productivity during Organisational Restructuring' (Masters thesis, University of New South Wales 2012)

Digital Industry Group Inc, *ACCC Digital Platforms Inquiry Final Report: Submission to Treasury* (12 September 2019) 14-23, available at <https://digi.org.au/wp-content/uploads/2017/02/DIGI-ACCC-DPI-Submission-to-Treasury-12-September-2019-FINAL.pdf> accessed 18 September 2019

DMDatabases, 'Ailments Mailing Lists/Email Lists' <http://dmdatabases.com/databases/consumer-mailing-lists/ailments-lists> accessed 30 June 2018

Donnelly T, 'Complete guide to the NBN: Your questions answered' (*WhistleOut*, 10 December 2018) <https://www.whistleout.com.au/Broadband/Guides/NBN-Guide-What-You-Need-to-Know> accessed 10 May 2019

doteveryone, *Regulating for Responsible Technology – Capacity, Evidence and Redress: A New System for a Fairer Future* (October 2018)

Dourish P and Bell G, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (MIT Press 2011)

Drahos P (ed), *Regulatory Theory: Foundations and Applications* (ANU Press 2017)

Dupont B, 'Bots, Cops, and Corporations: On the Limits of Enforcement and the Promise of Polycentric Regulation as a Way to Control Large-Scale Cybercrime' (2017) 67 Crime, Law and Social Change 97

Dynabook, 'dynaEdge™ AR Smart Glasses' <https://smartglasses.toshiba.com/> accessed 8 January 2019

Eberle EJ, 'The Methodology of Comparative Law' (2011) 16 Roger Williams University Law Review 51

ECHORD++ (European Coordination Hub for Open Robotics Development), 'MARS: Mobile Agricultural Robot Swarms' <http://echord.eu/mars/> accessed 23 February 2018

Eckhardt GM and Bengtsson A, 'A Brief History of Branding in China' (2009) 30 Journal of Macromarketing 210

Edara KK, 'Keyword Determinations from Voice Data' (*Google Patents*, 23 September 2011) <https://patents.google.com/patent/US8798995B1> accessed 1 July 2018

Edwards L, 'Data Protection: Enter the General Data Protection Regulation' in Edwards L (ed) *Law, Policy and the Internet* (Hart Publishing 2018)

Edwards L and Veale M, 'Slave to the Algorithm? Why a "Right to Explanation" Is Probably Not the Remedy You Are Looking for' (2017) 16 Duke Law & Technology Review 18

Edwards L and Waelde C (eds), *Law and the Internet: Regulating Cyberspace* (Hart Publishing 1997)

Eisen M, 'Amazon's $23,698,655.93 Book about Flies' (*it is NOT junk: a blog about genomes, DNA, evolution, open science, baseball and other important things*, 22 April 2011) <www.michaeleisen.org/blog/?p=358> accessed 3 January 2017

Elvy S-A, 'Contracting in the Age of the Internet of Things: Article 2 of the UCC and Beyond' (2016) 44 Hofstra Law Review 839

—— 'Hybrid Transactions and the Internet of Things: Goods, Services, or Software?' (2017) 74 Washington and Lee Law Review 77

Endres C, Butz A and MacWilliams A, 'A Survey of Software Infrastructures and Frameworks for Ubiquitous Computing' (2005) 1 Mobile Information Systems 41

EPCglobal Inc, 'EPCglobal' <www.gs1.org/standards/epc-rfid> accessed 14 October 2018

Epps SR, 'There Is No Internet of Things' (*Forbes*, 17 October 2013) <www.forbes.com/sites/forrester/2013/10/17/there-is-no-internet-of-things/> accessed 5 February 2018

Epstein RA, 'The Static Conception of the Common Law' (1980) 9 The Journal of Legal Studies 253

European Commission, A Digital Single Market Strategy for Europe COM (2015) 192 final (2015)

—— Amended Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods COM(2017) 637

—— Commission Staff Working Document Impact Assessment on the modernisation of EU copyright rules SWD(2016) 301 (Accompanying the document: Proposal for a Directive of the European Parliament and of the Council on copyright in the Digital Single Market and Proposal for a Regulation of the European Parliament and of the Council laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, 2016)

European Commission, Joint Research Centre, 'SWAMI Project: Safeguards in a World of Ambient Intelligence' (2005) <http://is.jrc.ec.europa.eu/pages/TFS/SWAMI.html> accessed 14 July 2018

—— 'Smart Grid Projects Outlook 2017' <https://ses.jrc.ec.europa.eu/smart-grids-observatory> accessed 9 September 2018

—— Report of Internet of Things Privacy and Security Workshop

Evans M and Jones B, *Equity and Trusts* (LexisNexis Butterworths 2012)

Explanatory Memorandum, Competition and Consumer Legislation Amendment Bill 2010 (Cth)

Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth)

Eyal N and Hoover R, *Hooked: How to Build Habit-Forming Products* (Portfolio/Penguin 2014)

Facebook, *Facebook's Response to the Digital Platforms Inquiry* (12 September 2019) 104-123, available at <https://fbnewsroomus.files.wordpress.com/2019/09/facebook-submission-to-treasury-on-digital-platforms-inquiry.pdf> accessed 15 September 2019

Facebook Newsroom, 'Comments on Research and Ad Targeting' (*Facebook*, 30 April 2017) <https://newsroom.fb.com/news/h/comments-on-research-and-ad-targeting/> accessed 28 August 2018

Fairfield J, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (2012) 27 Berkeley Technology Law Journal 55

Farrell J and Klemperer P, 'Coordination and Lock-in: Competition with Switching costs and Network Effects' in Armstrong M and Porter R (eds), *Handbook of Industrial Organization*, vol 3 (Elsevier BV 2007)

Federal Trade Commission, 'FTC Issues Warning Letters to App Developers Using "Silverpush" Code' (Press Release, 17 March 2016) <www.ftc.gov/news-events/press-releases/2016/03/ftc-issues-warning-letters-app-developers-using-silverpush-code> accessed 4 March 2018

Federal Trade Commission, *Cross-Device Tracking: An FTC Staff Report* (January 2017)

—— *Data Brokers: A Call for Transparency and Accountability* (May 2014)

—— *The Internet of Things: Privacy and Security in a Connected World* (January 2015)

Finch J, 'The Vignette Technique in Survey Research' (1987) 21 Sociology 105

Finn P, 'Common Law Divergences' (2013) 37 Melbourne University Law Review 509

Finn PD, *Essays in Equity* (Law Book Co 1985)

Firebox, 'iKettle: 3rd Gen' <https://www.firebox.com/iKettle-3rd-Gen/p8185> accessed 25 April 2019

Fitbit <www.fitbit.com/au/home> accessed 23 August 2018

—— 'Fitbit Privacy Policy' <www.fitbit.com/au/legal/privacy-policy> accessed 30 December 2014

Fiveash K, 'DeSENSORtised: Why the "Internet of Things" will FAIL without IPv6' (*The Register*, 14 April 2014) <www.theregister.co.uk/2014/04/24/ipv6_iot/> accessed 23 October 2018

Flear ML, 'Clinical Trials Abroad: The Marketable Ethics, Weak Protections and Vulnerable Subjects of EU Law' (2017) 16 Cambridge Yearbook of European Legal Studies 75

Flores A, Bechtel K and Lowenkamp C, 'False Positives, False Negatives, and False Analyses: A Rejoinder to "Machine Bias: There's Software Used across the Country to Predict Future Criminals. And It's Biased Against Blacks"' (2016) 80 Federal Probation 38

Fogg BJ, *Persuasive Technology: Using Computers to Change What We Think and Do* (Morgan Kaufmann Publishers 2003)

ForbrukerRadet (Norwegian Consumer Council), 'Connected Toys Violate European Consumer Law' <www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/> accessed 9 July 2018

Franceschi-Bicchierai L, 'A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them' (*Motherboard*, 3 February 2016)

<https://motherboard.vice.com/en_us/article/bmvnzz/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them > accessed 24 April 2019

Frantz D, 'Going Digital: Making the Transformation Work for Growth and Well-Being' (*OECD*, 24 January 2017) <www.oecd-forum.org/channels/722-digitalisation/posts/17393-going-digital-making-the-transformation-work-for-growth-and-well-being> accessed 11 June 2018

Friedewald M and others, 'Perspectives of Ambient Intelligence in the Home Environment' (2005) 22 Telematics and Informatics 221

—— 'The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues' in Clark JA and others (eds), *Security in Pervasive Computing* (SPC 2006 Lecture Notes in Computer Science, Springer 2006)

Furmston M, Tolhurst GJ and Mik E (contributor), *Contract Formation: Law and Practice* (2nd edn, OUP 2016)

Fussell S, 'The Microphones That May Be Hidden in Your Home' *The Atlantic* (23 February 2019) <www.theatlantic.com/technology/archive/2019/02/googles-home-security-devices-had-hidden-microphones/583387/> accessed 26 February 2019

Garmin, 'Menstrual cycle tracking' <https://connect.garmin.com/features/menstrual-cycle-tracking/> accessed 9 May 2019

Garreau J, *Radical Evolution: The Promise and Peril of Enhancing Our Minds, Our Bodies – And What It Means to Be Human* (Doubleday 2005)

Gasson MN, Kosta E and Bowman DM, *Human ICT Implants: Technical, Legal and Ethical Considerations* (Information Technology and Law Series, Springer 2012)

Gavaghan C, 'Lex Machina: Techno-Regulatory Mechanisms and Rules by Design' (2017) 15 Otago Law Review 123

Geetter J, 'Coding for Change: The Power of the Human Genome to Transform the American Health Insurance System' (2002) 28 American Journal of Law & Medicine 1

Geis GT, *Semi-Organic Growth: Tactics and Strategies Behind Google's Success* (Wiley 2015)

Genesis Toys, 'My Friend Cayla' <www.myfriendcayla.com/> accessed 5 September 2018

Gershenfeld N and Vasseur J, 'As Objects Go Online: The Promise (and Pitfalls) of the Internet of Things' (2014) 93 Foreign Affairs 60

Gershenfeld N, Krikorian R and Cohen D, 'The Internet of Things' (2004) Scientific American 76

Gervais DJ, 'The Regulation of Inchoate Technologies' (2010) 47 Houston Law Review 665

Gibbs S, 'iOS9 Making Your iPhone Slow? You're Not Alone' *The Guardian* (Sydney, 24 September 2015) <www.theguardian.com/technology/2015/sep/24/iphone-slow-ios-9-update-iphone-4s-iphone-5-iphone-5s> accessed 12 January 2017

Giblin R, 'Stranded in the Technological Dark Ages: Implications of the Full Federal Court's decision in NRL v Optus' (2012) 35 European Intellectual Property Review 632

Gibson W, 'Burning Chrome' in *Burning Chrome* (Harper Collins 1995)

Gill B and Smith D, *The Edge Completes the Cloud: A Gartner Trend Insight Report* (14 September 2018)

Giuffrida I, Lederer F and Vermeys N, 'A Legal Perspective on the Trials and Tribulations of AI: How Artificial Intelligence, the Internet of Things, Smart Contracts, and Other Technologies Will Affect the Law' (2018) 68 Case Western Reserve Law Review 747

Good Night Lamp <http://goodnightlamp.com/> accessed 24 August 2018

Goodloe K and Gallo MN, 'Senate Reintroduces IoT Cybersecurity Improvement Act' (*Global Policy Watch*, 13 March 2019) <https://www.globalpolicywatch.com/2019/03/senate-reintroduces-iot-cybersecurity-improvement-act/> accessed 7 April 2019

Goodwin M, 'Introduction: A Dimensions Approach to Technology Regulation' in Goodwin M, Koops B-J and Leenes R (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010)

Grand View Research, 'Internet of Things in Healthcare Market Size, Industry Report 2019–2025' (November 2018) <www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market> accessed 23 February 2019

Grauer Y, 'Dark Patterns Are Designed to Trick You (And They're All Over the Web)' (*arsTECHNICA*, 28 July 2016) <http://arstechnica.com/security/2016/07/dark-patterns-are-designed-to-trick-you-and-theyre-all-over-the-web/> accessed 1 May 2018

Greenfield A, *Everyware: The Dawning Age of Ubiquitous Computing* (New Riders 2006)

—— 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' (*Wired*, 21 July 2015) <www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/> accessed 1 September 2015

Greenberg A and Zetter K, 'How the Internet of Things Got Hacked' (*Wired*, 28 December 2015) <www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/>

Greenberg BA, 'Rethinking Technology Neutrality' (2016) 100 Minnesota Law Review 1495

Greenleaf G, 'Privacy Enforcement in Australia Is Strengthened: Gaps Remain' (2014) 128 Privacy Laws & Business International Report 1

Griggs L, 'Intervention or Empowerment: Choosing the Consumer Law Weapon!' (2007) 15 Competition & Consumer Law Journal

Griggs L and Webb E, 'Section 22 Unconscionability: A Sauropod in Need of Life Support' (2011) 11 Law and Justice Journal 31

Grubb B, 'Australia's Privacy Watchdog is "Woefully" and "Criminally" Underfunded' (*Crikey*, 16 July 2018) <www.crikey.com.au/2018/07/16/australias-privacy-watchdog-is-woefully-and-criminally-underfunded/?ft=SGxCKzkvcXRVNWkoeU1tcjdPcGlNQT09> accessed 14 February 2019

Grudin J, 'Group Dynamics and Ubiquitous Computing' (2002) 45 Communications of the ACM 74

Gulati R, Puranam P and Tushman M, 'Meta-Organization Design: Rethinking Design in Interorganizational and Community Contexts' (2012) 33 Strategic Management Journal 571

Hackers' List, 'Hacker for Hire FAQ' <https://hackerslist.com/FAQ.html> accessed 7 July 2018

HackersList, 'How it Works' <https://www.hackerslist.co/how-it-works/> accessed 24 April 2019

Hajian S, Bonchi F and Castillo C, 'Algorithmic Bias: From Discrimination Discovery to Fairness-Aware Data Mining' (Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, San Francisco, 13 August 2016)

Haller S, Karnouskos S and Schroth C, 'The Internet of Things in an Enterprise Context' in Domingue J, Fensel D and Traverso P (eds),

Future Internet: FIS 2008 (Lecture Notes in Computer Science vol 5468, Springer 2009)

Halliday J and Lam R, 'Internet of Things: Just Hype or the Next Big Thing?' (2015) 34 Communications Law Bulletin 7

—— 'Internet of Things: Just Hype or the Next Big Thing? Part II' (2016) 34 Communications Law Bulletin 4

Hamill J, 'Hackers Take Control of a Toilet Using Bog-Standard Computer Skills' *The Mirror* (London, 10 February 2016) <www.mirror.co.uk/tech/hackers-take-control-toilet-using-7342662> accessed 5 September 2018

Hansmann U, *Pervasive Computing: The Mobile World* (2nd edn, Springer 2003)

Hanson JD and Kysar DA, 'Taking Behavioralism Seriously: Some Evidence of Market Manipulation' (1999) 112 Harvard Law Review 1420

—— 'Taking Behavioralism Seriously: The Problem of Market Manipulation' (1999) 74 New York University Law Review 630

Harari YN, *Homo Deus: A Brief History of Tomorrow* (Harvill Secker 2016)

Harari YN and New Perspectives Quarterly, 'Dataism Is Our New God' (2017) 34 New Perspectives Quarterly 36

Hardingham IJ, 'Unconscionable Dealing' in Finn PD (ed), *Essays in Equity* (Law Book Co 1985)

Harper I and others, *Competition Policy Review: Final Report* (March 2015)

Hartzog W, 'Website Design as Contract' (2011) 60 American University Law Review 1635

Hartzog W and Selinger E, 'The Internet of Heirlooms and Disposable Things' (2016) 17 North Carolina Journal of Law & Technology 581

Heater B, 'Here's a Smart Hairbrush with a Built-In Microphone from Withings and L'Oreal' (*Techcrunch*, 3 January 2017) <https://techcrunch.com/2017/01/03/withings-brush/> accessed 15 November 2017

Helberger N, 'Profiling and Targeting Consumers in the Internet of Things: A New Challenge for Consumer Law' in Schulze R and Staudenmayer D (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Publishing 2016)

Heydon G and Zeichner F, *Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act* (Industry Report, Communications Alliance, October 2015)

Heydon JD, *Does Political Criticism of Judges Damage Judicial Independence?* (Policy Exchange Judicial Power Project Paper, February 2018)

—— *Trade Practices Law: Competition and Consumer Law* (Thomson Legal & Regulatory) (online version)

Higginbotham S, 'The Internet of Trash: IoT Has a Looming E-Waste Problem' (*IEEE Spectrum*, 29 May 2018) <https://spectrum.ieee.org/telecom/internet/the-internet-of-trash-iot-has-a-looming-ewaste-problem> accessed 7 September 2019.

Hildebrandt M, 'Algorithmic Regulation and the Rule of Law' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical, and Engineering Sciences

—— 'Law at a Crossroads: Losing the Thread or Regaining Control? The Collapse of Distance in Real-Time Computing' in Goodwin M, Koops B-J and Leenes R (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010)

—— *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing 2015)

Hildebrandt M and Koops BJ, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 Modern Law Review 428

Hill K, 'Watch Out, New Parents – Internet-Connected Baby Monitors Are Easy to Hack' (*Splinter*, 2 September 2015) <https://splinternews.com/watch-out-new-parents-internet-connected-baby-monitors-1793850489/> accessed 24 April 2019

—— 'Facebook Manipulated 689,003 Users' Emotions for Science' (*Forbes*, 28 June 2014) <www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#2f6a79e6197c> accessed 28 August 2018

Hillman R and Rachlinski J, 'Standard-Form Contracting in the Electronic Age', (2002) 77 *New York University Law Review* 429

Ho D and others, 'A Comparative Survey of Legal Awareness Between Hong Kong and Canadian Managers' (2013) 34 Company Lawyer 92

Hodgekiss A, 'Pacemaker Safety Alert: Thousands of Patients "At Risk of Serious Infection Because Battery Life Isn't Long Enough"' *Daily Mail Australia* (5 February 2016) <www.dailymail.co.uk/health/article-

3431734/Pacemaker-safety-alert-Thousands-patients-risk-infection-battery-life-isn-t-long-enough.html> accessed 4 November 2016

Hodson H, 'Inside China's Plan to Give Every Citizen a Character Score (Part One)' *New Scientist* (9 October 2015) <www.newscientist.com/article/dn28314-inside-chinas-plan-to-give-every-citizen-a-character-score/> accessed 12 October 2015

Hodson, J, 'NantHealth's Vitality Mobile App Now Available on Apple and Android Devices' (*Press Release*, 26 October 2017) <https://nanthealth.com/nanthealths-vitality-mobile-app-now-available-apple-android-devices/> accessed 24 August 2018

Hoffman S, 'Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease' in Cohen G, Hoffman A and Sage W (eds), *Big Data, Health Law, and Bioethics* (CUP 2018)

Hon WK, Millard C and Singh J, 'Twenty Legal Considerations for Clouds of Things' (Queen Mary School of Law, Legal Studies Research Paper No 216, 2016) <http://ssrn.com/abstract=2716966> accessed 14 July 2018

Horrigan B, Lieberman D and Steinwall R, *Strengthening Statutory Unconscionable Conduct and the Franchising Code of Conduct* (Expert Panel Report to the Treasury and the Department of Innovation, Science and Research, February 2010)

House of Lords Select Committee on Artificial Intelligence, *AI in the UK: Ready, Willing and Able?* (Report of Session 2017–19, HL Paper 100, 16 April 2018)

House of Lords Select Committee on Communications, *Regulating the Digital World* (2nd Report of Session 2017–19, HL Paper 299, 9 March 2019)

Howells GG and Weatherill S, *Consumer Protection Law* (Dartmouth 1995)

Hroncich C, 'Integrating Industrial Internet of Things and Pharmaceutical Manufacturing Processes' (2017) 41 Pharmaceutical Technology 46

Hubbard FP, '"Sophisticated Robots": Balancing Liability, Regulation, and Innovation' (2014) 66 Florida Law Review 1803

Human Rights Commission, *Human Rights and Technology* (Issues Paper, July 2018)

Hutchison T and Duncan N, 'Defining and Describing What We Do: Doctrinal Legal Research' (2012) 17 Deakin Law Review 83

Iansiti M and Levien R, 'Strategy as Ecology' (2004) 82 Harvard Business Review 68

Ibem EO and Laryea S, 'Survey of digital technologies in procurement of construction projects' (2014) 46 Automation in Construction 11

Information Society and Technology Advisory Group, *Ambient Intelligence: From Vision to Reality* (Report, European Commission, September 2003)

—— *Scenarios for Ambient Intelligence in 2010* (Final Report, European Commission Community Research, 2001)

—— *Strategic Orientations and Priorities for IST in FP6* (Report, European Commission, June 2002)

Ingress <www.ingress.com> accessed 9 September 2018

Inrix, 'Inrix' <http://inrix.com/> accessed 9 September 2018

IoT Alliance Australia, *Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia: V1.0* (November 2017)

—— *Internet of Things Security Guideline: V1.0* (February 2017)

—— *Internet of Things Security Guideline: V1.2* (November 2017)

ISO/IEC JTC 1, *Internet of Things (IoT): Preliminary Report 2014* (ISO 2015)

James N, 'Online Contracts, Electronic Signatures and the Law' (2000) 36 Australian Property Journal 283

Jenn-Air <https://jennair.com/connect> accessed 25 August 2018

Jessen PW and Henschel RF, 'Editorial: Special Issue on Legal Aspects of Mobile Commerce and Pervasive Computing: Privacy, Marketing, Contracting and Liability Issues' (2011) 4 International Journal of Private Law 185

John Deere, 'License Agreement for John Deere Embedded Software' (28 October 2016) <www.deere.com/privacy_and_data/docs/agreement_pdfs/english/2016-10-28-Embedded-Software-EULA.pdf> accessed 27 April 2017

Johnson DR and Post D, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367

Johnson T, 'Smart Billboards Are Checking You Out – And Making Judgments' *The Seattle Times* (Seattle, 26 September 2017) <www.seattletimes.com/business/smart-billboards-are-checking-you-out-and-making-judgments/> accessed 24 August 2018

Kagan RA, 'Understanding Regulatory Enforcement' (1989) 11 Law & Policy 89

Kang J, 'Information Privacy in Cyberspace Transactions' (1998) 50 Stanford Law Review 1193

Kang J and Cuff D, 'Pervasive Computing: Embedding the Public Sphere' (2005) 62 Washington and Lee Law Review 93

Kariyawasam, K and Wigley, S, 'Online Shopping, Misleading Advertising and Consumer Protection' (2017) 26 Information & Communications Technology Law 73

Kemp K, Email Correspondence with Author, 20 November 2018

Kidman A, 'Malcolm Turnbull: The Internet of Things Relies on Imagination, Not Regulation' (*Lifehacker*, 26 March 2015) <www.lifehacker.com.au/2015/03/malcolm-turnbull-the-internet-of-things-relies-on-imagination-not-regulation/> accessed 20 June 2016

Kim NS, 'Two Alternate Visions of Contract Law in 2025' (2014) 52 Duquesne Law Review 303

—— *Wrap Contracts: Foundations and Ramifications* (OUP 2013)

Kinder KE, 'Ubiquitous Computing in Industrial Workplaces: Cultural Logics and Theming in Use Contexts' (PhD thesis, Lancaster University 2009)

Kirby M, 'The Fundamental Problem of Regulating Technology' (2009) 5 The Indian Journal of Law and Technology 1

Kirilenko A and others, 'The Flash Crash: High-Frequency Trading in an Electronic Market' (2017) 72 Journal of Finance 967

Kitchin R, *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences* (Sage 2014)

Kitchin R and Dodge M, *Code/Space: Software and Everyday Life* (Software Studies, MIT Press 2011)

Klang M, 'Disruptive Technology: Effects of Technology Regulation on Democracy' (Goteburg University 2006)

Klein HK and Kleinman DL, 'The Social Construction of Technology: Structural Considerations' (2002) 27 Science, Technology, & Human Values 28

Knapp CL, 'Rescuing Reliance: The Perils of Promissory Estoppel' (1998) 49 Hastings Law Journal 1191

Knight W, 'The Dark Secret at the Heart of AI' (2017) 120 MIT Technology Review 54

Koebler J, 'Why American Farmers Are Hacking Their Tractors with Ukrainian Firmware' (*Motherboard*, 22 March 2017)

<https://motherboard.vice.com/en_us/article/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware> accessed 1 May 2017

Kohn MM and others, 'SMART CAMP: Environmental Sustainability through Intelligent Automation Technologies' (24th IEEE International Conference on Advanced Information Networking and Applications, Perth, 20–23 April 2010)

Koops B-J, 'Should ICT Regulation Be Technology Neutral?' in Koops B-J and others (eds), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners* (TMC Asser Press 2006)

—— 'Ten Dimensions of Technology Regulation: Finding Your Bearings in the Research Space of an Emerging Discipline' in Goodwin M, Koops B-J and Leenes R (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing 2010)

Kramer ADI, Guillory JE and Hancock JT, 'Experimental Evidence of Massive-Scale Emotional Contagion through Social Networks' (2014) 111 Proceedings of the National Academy of Sciences 8788

Kranz M, 'What We Can Learn from China About IoT' (Forbes, 5 March 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/03/05/what-we-can-learn-from-china-about-iot/#36872d9237af> accessed 30 June 2018.

Krebs B, 'KrebsOnSecurity Hit with Record DDoS' (*KrebsOnSecurity*, 21 September 2016) <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/> accessed 24 October 2016

Landi H, 'Report: Ransomware Attacks on IoT Medical Devices Will Likely Increase' (*Healthcare Informatics*, 29 November 2016) <www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware> accessed 13 January 2017

Langemeyer I, 'Contradictions in Expansive Learning: Towards a Critical Analysis of Self-Dependent Forms of Learning in Relation to Contemporary Socio-Technological Change' (2006) 7 Forum: Qualitative Social Research Art 12

Larson J and others, 'How We Analyzed the COMPAS Recidivism Algorithm' (*ProPublica*, 23 May 2016) <www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm> accessed 8 July 2018

Lasse Lueth K, 'State of the IoT 2018: Number of IoT Devices Now at 7B – Market Accelerating' (*IoT Analytics*, 8 August 2018) <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/> accessed 14 February 2019

Laughlin A, 'Which? Investigation Reveals "Staggering" Level of Smart Home Surveillance' (*Which?* 1 June 2018) <www.which.co.uk/news/2018/06/which-investigation-reveals-staggering-level-of-smart-home-surveillance/> accessed 30 June 2018

Laukyte M, 'Artificial Agents Among Us: Should We Recognize Them as Agents Proper?' (2017) 19 Ethics and Information Technology 1

Lawrence K, 'Should the Internet of Vibrating Things Be Worried?' (*Readwrite*, 13 October 2016) <http://readwrite.com/2016/10/13/should-the-internet-of-vibrating-things-be-worried-dl1/> accessed 6 December 2016

Leenes R, 'Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology' (2011) 5 Legisprudence 143

Leff AA, 'Unconscionability and the Code: The Emperor's New Clause' (1967) 115 University of Pennsylvania Law Review 485

Leith P, 'A Note on Using Vignettes in Socio-Legal Research' (2013) 19 Web Journal of Current Legal Issues

LeMay R, 'Locked Down: Foxtel Blocks Non-Samsung Android, Jailbroken Apple Devices' (*Delimiter*, 17 July 2013) <https://delimiter.com.au/2013/07/17/locked-down-foxtel-blocks-non-samsung-android-jailbroken-apple-devices/> accessed 30 June 2018

Leonard P, 'A Review of Australian Privacy Commissioner v Telstra Corporation Limited' (*Gilbert + Tobin Lawyers*, 16 February 2017) <www.gtlaw.com.au/insights/review-australian-privacy-commissioner-v-telstra-corporation-limited> accessed 16 January 2019

Lepawsky L, 'Beyond Recycling: solving e-waste problems must include designers and consumers' (*The Conversation,* 28 May 2015), <https://theconversation.com/beyond-recycling-solving-e-waste-problems-must-include-designers-and-consumers-41719> accessed 4 September 2019.

Lessig L, *Code 2.0* (Basic Books 2006)

—— *Code and Other Laws of Cyberspace* (Basic Books 1999)

Leveson NG and Turner CS, 'An Investigation of the Therac-25 Accidents' (1993) 26 Computer 18

LexisNexis, *Halsbury's Laws of Australia* (online looseleaf) (LexisNexis 2013)

Leydon J, 'Anti-Ultrasound Tech Aims to Foil the Dog-Whistle Marketeers' (*The Register*, 4 November 2016) <www.theregister.co.uk/2016/11/04/marketing_privacy/> accessed 30 January 2018

LG <www.lg.com/us/discover/smartthinq/refrigerators> accessed 5 September 2018

Li G, 'Deciphering Pervasive Computing: A Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' in Godara V (ed), *Risk Assessment and Management in Pervasive Computing: Operational, Legal Ethical and Financial Perspectives* (Information Science Reference 2009)

—— 'What We Know and Do Not Know: The Legal Challenges for International Commercial Contract Formation in a Pervasive Computing Environment' (2011) 4 International Journal of Private Law 252

Localz, 'Localz' <https://localz.com/customer-stories/> accessed 9 September 2018

Lockhart C, *The Law of Misleading or Deceptive Conduct* (4th edn, LexisNexis Butterworths 2015)

—— *The Law of Misleading or Deceptive Conduct* (5th edn, LexisNexis Butterworths 2019)

Lyytinen K and Yoo Y, 'Issues and Challenges in Ubiquitous Computing' (2002) 45 Communications of the ACM 62

Lyytinen K and others, 'Surfing the Next Wave: Design and Implementation Challenges of Ubiquitous Computing' (2004) 30 Communications of the Association for Information Systems 695

Macdonald B, 'Legislative Intervention in the Law of Negligence: The Common Law, Statutory Interpretation and Tort Reform in Australia' (2005) 27 Sydney Law Review 443

MacKenzie D and Wajcman J (eds), *The Social Shaping of Technology: How the Refrigerator Got Its Hum* (2nd edn, Open UP 1999)

Maeda E and Minami Y, 'Steps Towards Ambient Intelligence' (2006) 4 NTT Technical Review 50

Maheshwari S, 'Hey, Alexa, What Can You Hear? And What Will You Do with It?' *The New York Times* (New York, 31 March 2018)

<www.nytimes.com/2018/03/31/business/media/amazon-google-privacy-digital-assistants.html> accessed 4 April 2018

Mak V, 'Contract and Consumer Law' in Mak V, Tjong Tjin Tai E and Berlee A (eds), *Research Handbook in Data Science and Law* (Edward Elgar 2018)

Malbon J and Nottage L, *Consumer Law and Policy in Australia and New Zealand* (Federation Press 2013)

Mandel GN, 'Legal Evolution in Response to Technological Change' in Brownsword R, Scotford E and Yeung K (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017)

Mann S, 'Wearable Computing' in Soegaard M and Dam RF (eds), *The Encyclopedia of Human-Computer Interaction* (2nd edn, The Interaction Design Foundation 2012)

Manwaring K, 'A Shift in Time Saves No-One: Mobile Technologies and the NRL v Optus Decision' (2012) 5 Journal of the Australasian Law Teachers Association 83

—— 'Canning the Spam Five Years On: A Comparison of Spam Regulation in Australia and the US' (2009) 76 Computers & Law 5

—— 'Data Breach Notifications: An Australian Perspective' (2009) Privacy and Data Security Law Journal 848

—— 'Digital Consumer Manipulation Enabled by Emerging Technologies' (British and Irish Law Education and Technology Association Conference, Aberdeen, April 2018)

—— 'Emerging Information Technologies: Challenges for Consumers' (2017) 17 Oxford University Commonwealth Law Journal 265

—— 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the US and the UK' (2011) 5 Studies in Ethics, Law, and Technology Article 4

—— 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 Deakin Law Review 51

—— 'Network Neutrality: Issues for Australia' (2010) 26 Computer Law and Security Review 630

—— 'Surfing the Third Wave of Computing: Contracting with eObjects' (Proceedings DCIT 2016, Doctoral Consortium on Internet of Things, First International Conference on Internet of Things and Big Data 2016, Rome, 22–25 April 2016)

—— 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (Law, Technology & Innovation Junior Scholars Forum, UNSW Kensington, 24 November 2017)

—— 'Will Emerging Information Technologies Outpace Consumer Protection Law? The Case of Digital Consumer Manipulation' (2018) 26 Competition and Consumer Law Journal 141

—— 'A Legal Analysis of Socio-Technological Change Arising Out of eObjects' (UNSW Law Research Paper No 2016–15, 2015) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2690024> accessed 18 May 2018

Manwaring K and Clarke R, 'Surfing the Third Wave of Computing: A Framework for Research into eObjects' (2015) 31 Computer Law & Security Review 586

Marchant GE, Allenby BR and Herkert JR (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer 2011)

Markets and Markets, 'IoT Healthcare Market Worth 163.24 Billion USD by 2020' <www.marketsandmarkets.com/PressReleases/iot-healthcare.asp> accessed 7 July 2018

Markovits D, 'Contract and Collaboration' (2004) 113 Yale Law Journal 1417

Marks G, 'How Google Saved Google Glass' (*Forbes*, 2 February 2012) <www.forbes.com/sites/quickerbettertech/2015/02/02/how-google-saved-google-glass/> accessed 4 February 2015

Marks M, Letter from Melanie Marks to Rob Nicholls (18 April 2019)

Martin A, 'Step and Save: The Truth about Wearables and Health Insurance' (*Wareable*, 21 May 2015) <www.wareable.com/wearable-tech/step-and-save-the-risks-of-using-fitness-tracker-to-save-on-your-insurance-premium-1163> accessed 3 November 2016

Martinez AF, 'The Noisy Fallacies of Psychographic Targeting' (*Wired*, 19 March 2018) <www.wired.com/story/the-noisy-fallacies-of-psychographic-targeting/> accessed 30 June 2018

Mason A, 'The Place of Equity and Equitable Remedies in the Contemporary Common Law World' (1994) 110 Law Quarterly Review 238

Mathews-Hunt K, 'ConsumeR-IOT: Where Every Thing Collides. Promoting Consumer Internet of Things Protection in Australia' (SJD minor thesis, Bond University 2017)

—— 'CookieConsumer: Tracking Online Behavioural Advertising in Australia' (2016) 32 Computer Law & Security Review 55

Matz SC and others, 'Psychological Targeting as An Effective Approach to Digital Mass Persuasion' (Proceedings of the National Academy of Sciences of the USA, 28 November 2017)

Maurushat A, 'Zombie Botnets' (2010) 7(2) Scripted 370

McConville M and Chui WH, *Research Methods for Law* (Edinburgh UP 2007)

McCue T, '$117 Billion Market for Internet of Things in Healthcare By 2020' (*Forbes*, 22 April 2015) <www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/#26c66b5f2471>

McKerchar M, *Design and Conduct of Research in Tax, Law and Accounting* (Thomson Reuters/Lawbook Co 2010)

McLeod S, 'Statutory Unconscionable Conduct under the ACL: The Case Against a Requirement for "Moral Obloquy"' (2015) 23 Competition and Consumer Law Journal 123

McMahon C, 'iPromise: How Contract Theory Can Inform Regulation of Online Consumer Contracts' (2018) 21 Trinity College Law Review 174

Medtronic <www.medtronic-diabetes.com.au> accessed 23 August 2018

Meeroona, '17 Portable Health Gadgets That Can Change Your Life' (*Travel Away*, 13 November 2018) <https://travelaway.me/portable-health-gadgets/> accessed 22 December 2018

Memorandum of Law in Support of Amazon's Motion to Quash Search Warrant in Arkansas v Bates (Circuit Court of Benton County, Arkansas, Case No Cr-2016-370-2, 17 February 2017)

Mesthene EG, *Technological Change: Its Impact on Man and Society* (Harvard UP 1970)

Meulendijk M and others, 'AmI in Good Care? Developing Design Principles for Ambient Intelligent Domotics for Elderly' (2011) 36 Informatics for Health and Social Care 75

Michael K and Michael MG (eds), *Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies* (Advances in Human and Social Aspects of Technology, Information Science Reference 2014)

Mide Technology, 'Piezoelectric Energy Harvesters' <https://piezo.com/collections/piezoelectric-energy-

harvesters?_=pf&pf_t_quantity=Quantity__1> accessed 23 February 2019

Mik E, 'The Erosion of Autonomy in Online Consumer Transactions' (2016) 8 Law, Innovation and Technology 1

Millard C, Hon WK and Singh J, 'Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities' (Proceedings of the 2017 IEEE International Conference on Cloud Engineering, Vancouver, 4-7 April 2017)

Miller AR, *The Assault on Privacy: Computers, Data Banks, and Dossiers* (Michigan UP 1971)

Miller RV, *Miller's Australian Competition and Consumer Law Annotated* (Thomson Reuters 2016)

Ministers for the Department of Industry Innovation and Science Senator Matt Canavan and Karen Andrews MP and Minister for Education Senator Simon Birmingham, 'Funding to Advance New Scientific and Technological Developments' (Media Release, 21 May 2018) <www.minister.industry.gov.au/ministers/cash/media-releases/funding-advance-new-scientific-and-technological-developments> accessed 14 November 2018

MIT Project Oxygen, *Pervasive, Human-Centred Computing* <oxygen.lcs.mit.edu/> accessed 28 August 2018

Montgomery-Downs H, Insana S and Bond J, 'Movement Toward a Novel Activity Monitoring Device' (2012) 16 Sleep Breath 913

Morgan B and Yeung K, *An introduction to law and regulation: text and materials* (Cambridge University Press 2007)

Morgan D, 'Technology in the Age of Anxiety: The Moral Economy of Regulation' (2009) 29 Legal Studies 492

Morgan J, 'Torts and Technology' in Brownsword R and others (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017)

Moringiello JM and Reynolds WL, 'From Lord Coke to Internet Privacy: The Past, Present, and Future of the Law of Electronic Contracting' (2013) 72 Maryland Law Review 452

Muaremi A, Arnrich B and Tröster G, 'Towards Measuring Stress with Smartphones and Wearable Devices during Workday and Sleep' (2013) 3 BioNanoScience 172

Murray AD, 'Mapping the Rule of Law for the Internet' in Gillies L and Mangan D (eds), The Legal Challenges of Social Media (Edward Elgar Publishing 2017)

—— *The Regulation of Cyberspace: Control in the Online Environment* (Routledge-Cavendish 2007)

Nadler A and McGuigan L, 'An Impulse to Exploit: The Behavioral Turn in Data-Driven Marketing' (2018) 35 Critical Studies in Media Communication 151

National Conference of Commissioners on Uniform State Laws, 'Computer Information Transactions Act' (15 October 2002) <https://my.uniformlaws.org/viewdocument/final-act-with-comments-14?CommunityKey=92b2978d-585f-4ab6-b8a1-53860fbb43b5&tab=librarydocuments> accessed 22 December 2018

National Intelligence Council, *Disruptive Technologies Global Trends 2025: Six Technologies with Potential Impacts on US Interests out to 2025* (Conference Report, CR 2008-7, April 2008)

Neato, 'Botvac™ Connected: The Ultimate Navigating Wi-Fi Connected Robot Vacuum' <www.neatorobotics.com/robot-vacuum/botvac-connected-series/botvac-connected/> accessed 23 August 2018

Nest <https://nest.com/smoke-co-alarm/overview/> accessed 25 August 2018

Nguyen P and Solomon L, *Consumer Data and the Digital Economy: Emerging Issues in Data Collection, Use and Sharing* (Consumer Policy Research Centre, July 2018)

Nilsson VT, 'You're Not from Around Here, Are You? Fighting Deceptive Marketing in the Twenty-First Century' (2012) 54 Arizona Law Review 801

Noldus, 'Philips HomeLab' <www.noldus.com/default/philips-homelab> accessed 9 September 2018

Nordrum A, 'Popular Internet of Things Forecast of 50 Billion Devices by 2020 is Outdated' (*IEEE Spectrum*, 18 August 2016) <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated> accessed 26 September 2018

Noto La Diega G and Walden I, 'Contracting for the "Internet of Things": Looking into the Nest' (2016) 7 European Journal of Law and Technology

—— 'Clouds of Things: Data Protection and Consumer Law at the Intersection of Cloud Computing and the Internet of Things in the United Kingdom' (2016) 9 Journal of Law and Economic Regulation 69

O'Connell B, 'Telematics Could Cut Your Car Insurance, But There Are Privacy Risks' (*The Street*, 21 February 2018) <www.thestreet.com/story/14493364/1/telematics-could-cut-your-car-insurance-but-there-are-privacy-risks.html> accessed 11 July 2018

O'Sullivan T, 'The Definition of "Consumer": Will the Real "Consumer" Please Stand up' (2016) 24 Competition & Consumer Law Journal 23

Obaidat MS, Denko M and Woungang I (eds), *Pervasive Computing and Networking* (John Wiley & Sons 2011)

Office of the Australian Information Commissioner, 'Determinations' <www.oaic.gov.au/privacy-law/determinations/> accessed 24 April 2018

Ogden GL, 'The Problem Method in Legal Education' (1984) 34 Journal of Legal Education 654

Ohm P, 'The Argument Against Technology-Neutral Surveillance Laws' (2010) 88 Texas Law Review 1685

Oliveira LM and Rodrigues JJ, 'Wireless Sensor Networks: A Survey on Environmental Monitoring' (2011) 6 Journal of Communications 143

Open Web Application Security Project (OWASP), 'OWASP Internet of Things Project' (2014) <www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29> accessed 12 January 2017

Oremus W, 'Smart Socks May Be the Future of Wearable Technology' *The Sydney Morning Herald* (Sydney, 30 November 2013) <www.smh.com.au/digital-life/digital-life-news/smart-socks-may-be-the-future-of-wearable-technology-20131130-2yihx.html>

Organisation for Economic Co-operation and Development (OECD), 'Going Digital: Making the Transformation Work for Growth and Well-Being' (*OECD*) <www.oecd.org/going-digital/project/> accessed 31 July 2018

—— *Consumer Policy and the Smart Home* (OECD Digital Economy Papers No 268, April 2018)

—— *Consumer Policy Toolkit* (June 2010)

—— *Consumer Product Safety in the Internet of Things* (OECD Digital Economy Papers No 267, March 2018)

—— *Going Digital in a Multilateral World: An Interim Report to Ministers* (Meeting of the OECD Council at Ministerial Level, Paris, 30–31 May 2018)

Orlikowski WJ and Gash DC, 'Technological Frames: Making Sense of Information Technology in Organisations' (1994) 12 ACM Transactions on Information Systems 174

Paez M and Tobitsch K, 'The Industrial Internet of Things: Risks, Liabilities, and Emerging Legal Issues' (2018) 62 New York Law School Law Review 217

Palmerini E and others, *Robolaw – D6.2: Guidelines on Regulating Robotics* (2014)

Parliamentary Office of Science and Technology <https://www.parliament.uk/post> accessed 9 May 2019

Pasquale F, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard UP 2015)

Paterson J and Brody G, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) 38 Journal of Consumer Policy 331

Payteck, 'Welcome to Payteck' <www.payteck.cc/> accessed 24 August 2018

Pearce D, Campbell E and Harding D, *Australian Law Schools: A Discipline Assessment for the Commonwealth Tertiary Education Commission* (1987)

Pearson G, 'The Ambit of Unconscionable Conduct in Relation to Financial Services' (2005) 23 Company and Securities Law Journal 105

Pebble, 'Pebble's Next Step' (7 December 2016) <https://blog.getpebble.com/2016/12/07/fitbit/#more-1032> accessed 11 July 2018 (had been shut down as of 24 April 2019)

Peeters R and Schuilenburg M, 'Machine Justice: Governing Security through the Bureaucracy of Algorithms' (2018) 23 Information Polity 267

Peppet SR, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (2012) 59 UCLA Law Review 676

—— 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85

Pew Research Center, 'US Smartphone Use in 2015' <www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/> accessed 4 June 2015

—— *The Internet of Things Connectivity Binge: What Are the Implications?* (June 2017)

PHDmedia, 'New Beauty Study Reveals Days, Times and Occasions When US Women Feel Least Attractive' (*Cision PR Newswire*, 2 October 2013) <www.prnewswire.com/news-releases/new-beauty-study-reveals-days-times-and-occasions-when-us-women-feel-least-attractive-226131921.html> accessed 1 January 2016

Pimple KD, 'Introduction: The Impacts, Benefits and Hazards of PICT' in Pimple KD (ed), Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities and Safeguards (Springer 2014)

Pointr, 'Beacons: Everything You Need to Know' <www.pointrlabs.com/posts/beacons-everything-you-need-to-know/> accessed 5 September 2018

Pokemon Go <www.pokemongo.com> accessed 9 September 2018

Polinsky AM, *An Introduction to Law and Economics* (4th edn, Wolters Kluwer Law & Business 2011)

Poole I, 'RFID History' (*Radio-Electronics.com*) <www.radio-electronics.com/info/wireless/radio-frequency-identification-rfid/development-history.php> accessed 20 February 2015

Poslad S, *Ubiquitous Computing: Smart Devices, Environment and Interaction* (John Wiley & Sons Ltd 2009)

Posner R, 'Law and Public Order in Space (Book Review)' (1964) 77 Harvard Law Review 1370

—— *The Problems of Jurisprudence* (Harvard UP 1990)

Power R and others, 'Scenario Planning Case Studies Using Open Government Data' in Denzer R and others (eds), *Environmental Software Systems: Infrastructures, Services and Applications* (Springer 2015)

Press G, 'It's Official: The Internet of Things Takes Over Big Data as the Most Hyped Technology' (*Forbes*, 18 August 2014) <www.forbes.com/sites/gilpress/2014/08/18/its-official-the-internet-of-things-takes-over-big-data-as-the-most-hyped-technology/#10c29f111aaa> accessed 27 August 2018

Price ME, 'The Newness of New Technology' (2001) 22 Cardozo Law Review 1885

Productivity Commission, *Data Availability and Use* (Productivity Commission Inquiry Report No 82, March 2017)

—— *Review of Australia's Consumer Policy Framework* (Productivity Commission Inquiry Report No 45, April 2008) 2 vols

Qin L, He X and Zhou DH, 'A Survey of Fault Diagnosis for Swarm Systems' (2014) 2 Systems Science & Control Engineering 13

Rabbinge R and Vanoijen M, 'Scenario Studies for Future Agriculture and Crop Protection' (1997) 103 European Journal of Plant Pathology 197

Radin M, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton UP 2013)

—— 'The Deformation of Contract in the Information Society (2016 HLA Hart Memorial Lecture)' (2017) 37 Oxford Journal of Legal Studies 505

Rahman M, Carbunar B and Banik M, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) arXiv:13045672 [csCR]

Ramachandran G, 'Against the Right to Bodily Integrity: Of Cyborgs and Human Rights' (2010) 87 Denver University Law Review 1

Razook N, 'The Politics and Promise of UCITA (Uniform Computer Information Transactions Act)' (2003) 36 Creighton Law Review 643

Reddy T, '15 Companies from Airports to Retail Already Using Beacon Technology' <www.umbel.com/blog/mobile/15-companies-using-beacon-technology/> accessed 10 November 2014

Reed C, 'How to Make Bad Law: Lessons from Cyberspace' (2010) 73 Modern Law Review 903

—— *Making Laws for Cyberspace* (OUP 2012)

—— 'Taking Sides on Technology Neutrality' (2007) 4 SCRIPTed 263

Reema S, 'Shifting Paradigm from Mobile to Ubiquitous/Pervasive Computing' (2013) 2 COMPUSOFT: International Journal of Advanced Computer Technology 360

Reich N, 'Diverse Approaches to Consumer Protection Philosophy' (1992) 14 Consumer Issues in Law, Economics and Behavioural Sciences 257

Reidenberg JR and others, 'Ambiguity in Privacy Policies and the Impact of Regulation' (2016) 45 The Journal of Legal Studies S163

Reitz JC, 'How to Do Comparative Law' (1998) 46 American Journal of Comparative Law 617

Rejeski D, 'Public Policy on the Technological Frontier' in Marchant GE, Allenby BR and Herkert JR (eds), *The Growing Gap Between Emerging*

Technologies and Legal-Ethical Oversight: the Pacing Problem (Springer 2011)

Richardson M and others, 'Privacy and the Internet of Things' (2016) 21 Media & Arts Law Review 336

—— 'Towards Responsive Regulation of the Internet of Things: Australian Perspectives' (2017) 6 Internet Policy Review

Rickett C, 'Unconscionability and Commercial Law' (2005) 24 University of Queensland Law Journal 73

Rico DF, Sayani HH and Field RF, 'History of Computers, Electronic Commerce and Agile Methods' (December 2008) 73 Advances in Computers 1

Ridge J, 'What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive' (2007–08) 49 South Texas Law Review 725

Riemer K and Vehring N, 'Virtual or Vague? A Literature Review Exposing Conceptual Differences in Defining Virtual Organizations in IS Research' (21st Bled eConference: eCollaboration: Overcoming Boundaries Through Multi-Channel Interaction, Bled, Slovenia, 15–18 June 2008)

Riva G and others, 'Presence 2010: The Emergence of Ambient Intelligence' in Riva G, Davide F and IJsselsteijn WA (eds), *Being There: Concepts, Effects and Measurements of User Presence in Synthetic Environments* (IOS Press 2003)

Roberti M, 'The History of RFID Technology' (*RFID Journal*, 16 January 2005) <www.rfidjournal.com/articles/view?1338/> accessed 26 February 2015

Roberts JJ, 'Privacy Groups Claim These Popular Dolls Spy on Kids' (*Fortune*, 8 December 2016) <http://fortune.com/2016/12/08/my-friend-cayla-doll/> accessed 20 November 2017

Robertson A, 'The Limits of Voluntariness in Contract' (2005) 29 Melbourne University Law Review 179

Romero-Moreno F, '"Notice and Staydown" and Social Media: Amending Article 13 of the Proposed Directive on Copyright' (2018) 32 International Review of Law, Computers & Technology 1

Rose K, Eldridge S and Chapin L, *The Internet of Things: An Overview. Understanding the Issues and Challenges of a More Connected World* (Internet Society, October 2015)

Rothchild J, 'Protecting the Digital Consumer: The Limits of Cyberspace Utopianism' (1999) 74 Indiana Law Journal 893

Roux T, 'Judging the Quality of Legal Research: A Qualified Response to the Demand for Greater Methodological Rigour' (2014) 24 Legal Education Review 173

Sadler D, 'Privacy Office at Breaking Point' (*InnovationAus*, 26 March 2018) <www.innovationaus.com/2018/03/Privacy-office-at-breaking-point> accessed 5 March 2018

Saha D and Mukherjee A, 'Pervasive Computing: A Paradigm for the 21st Century' (2003) 36 Computer 25

Samsung <www.samsung.com/us/explore/smart-tv/highlights/> accessed 25 August 2018

Sanchez Lopez T, 'What the Internet of Things is NOT' (*Technical Blog,* 22 March 2010) <http://technicaltoplus.blogspot.com.au/2010/03/what-internet-of-things-is-not.html> accessed 1 June 2017

Santucci G, 'From Internet of Data to Internet of Things' (International Conference on Future Trends of the Internet, Luxembourg, 28 January 2009)

Sarewitz D, 'Anticipatory Governance of Emerging Technologies' in Marchant GE, Allenby BR and Herkert JR (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: the Pacing Problem* (Springer 2011)

Sartor G, 'Cognitive Automata and the Law: Electronic Contracting and the Intentionality of Software Agents' (2009) 17 Artificial Intelligence and Law 253

Satyanarayanan M, 'Fundamental Challenges in Mobile Computing' (1996) Principles of Distributed Computing: Proceedings of the Fifteenth Annual ACM Symposium 1

—— 'Pervasive Computing: Vision and Challenges' (2001) 8 IEEE Personal Communications 10

Saunders G, 'My Flamboyant Grandson' *The New Yorker* (28 January 2002) 78

Sax M, Helberger N and Bol N, 'Health as a Means Towards Profitable Ends: mHealth Apps, User Autonomy, and Unfair Commercial Practices' (2018) 41 Journal of Consumer Policy 103

Schaffarczyk K, 'Explainer: What is Geoblocking?' (*The Conversation*, 17 April 2013) <http://theconversation.com/explainer-what-is-geoblocking-13057> accessed 3 May 2016

Schellekens M, 'Self-Driving Cars and the Chilling Effect of Liability Law' (2015) 31 Computer Law & Security Review 506

Schmidt A, 'Implicit Human Computer Interaction through Context' (2000) 4 Personal Technologies 191

—— 'Ubiquitous Computing: Computing in Context' (PhD thesis, Lancaster University 2002)

Schneier B, 'The Internet of Things Is Wildly Insecure: And Often Unpatchable' (*Wired*, 1 June 2014) <www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/> accessed 17 December 2015

Schon DA, *Technology and Change: The New Heraclitus* (Delacorte Press 1967)

Schwartz PM and Solove DJ, 'The PII Problem: Privacy and a New Concept of Personally Identifiable Information' (2011) 86 New York University Law Review 1814

Scott RE and Kraus JS, *Contract Law and Theory* (5th edn, LexisNexis 2013)

Second Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No 2) 2010 (Cth)

Security Ledger, 'Update: Hello Barbie Fails Another Security Test' (*SecurityLedger*, 4 December 2015) <https://securityledger.com/2015/12/hello-barbie-fails-another-security-test/> accessed 17 December 2015

Selznick P, 'Focusing Organisational Research on Regulation' in Noll R (ed) *Regulatory Policy and the Social Sciences* (California UP 1985)

Sensoria <www.sensoriafitness.com/> accessed 10 September 2018

Serrano E and Botia J, 'Validating Ambient Intelligence Based Ubiquitous Computing Systems by Means of Artificial Societies' (2013) 222 Information Sciences 3

Shaban H, 'An Amazon Echo Recorded a Family's Conversation, Then Sent it to a Random Person in their Contacts, Report Says' *Washington Post* (Washington, 24 May 2018) <www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says> accessed 30 May 2018

Sharpe M and Parker C, 'A Bang or a Whimper? The Impact of ACCC Unconscionable Conduct Enforcement' (2007) 15 Trade Practices Law Journal 139

Simonite T, 'Google Glass is Back: Now with Artificial Intelligence' (*Wired*, 25 July 2018) <www.wired.com/story/google-glass-is-backnow-with-artificial-intelligence/> accessed 25 July 2018

Singer N, 'Listen to Pandora, and It Listens Back' *New York Times* (New York, 4 January 2014) <www.nytimes.com/2014/01/05/technology/pandora-mines-users-data-to-better-target-ads.html> accessed 21 October 2017

Singh J and others, 'Accountability in the IoT: Systems, Law, and Ways Forward' (2018) 51 Computer 54

Singh S, Puradkar S and Lee Y, 'Ubiquitous Computing: Connecting Pervasive Computing through Semantic Web' (2006) 4 Information Systems and e-Business Management 421

Smart Homes <www.smarthomes.com.au> accessed 24 August 2018

Smart Start Interlocks <www.smartstartinterlocks.com.au/products.html> accessed 23 August 2018

Smith SA, *Contract Theory* (OUP 2004)

Snell J and Lee C, 'The Internet of Things Changes Everything, or Does it? Your Handy Guide to Legal Issue-Spotting in a World Where Everything is Connected' (2015) 32 The Computer & Internet Lawyer

Solove DJ, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880

Soltan S, Mittal P and Poor HV, 'BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid' (Proceedings of the 27th USENIX Security Symposium, 15–17 August 2018, Baltimore)

Sony, 'Support' (13 July 2017) <https://esupport.sony.com/US/p/news-item.pl?news_id=519> accessed 23 September 2018

Stone B, 'Amazon Erases Orwell Books from Kindle' *The New York Times* (New York, 18 July 2009) <www.nytimes.com/2009/07/18/technology/companies/18amazon.html> accessed 18 May 2016

Stucke ME and Ezrachi A, 'How Digital Assistants Can Harm Our Economy, Privacy, and Democracy' (2017) 32 Berkeley Technology Law Journal 1239

Sunstein C, 'Fifty Shades of Manipulation' (2016) 1 Journal of Marketing Behaviour 213

Super DA, 'Against Flexibility' (2011) 96 Cornell Law Review 1375

Surden H and Williams M-A, 'Technological Opacity, Predictability, and Self-Driving Cars' (2016) 38 Cardozo Law Review 181

Svantesson DJB, 'A Legal Method for Solving Issues of Internet Regulation' (2011) 19 International Journal of Law and Information Technology 243

Swan M, 'Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0' (2012) 1 Journal of Sensor and Actuator Networks 217

Swinson M, Osborn W and Swan S, 'There's a Glitch in the Matrix: The Application of Consumer Guarantees to the IoT" (November 2017) Inhouse Counsel

Tapper C, 'Judicial Attitudes, Aptitudes and Abilities in the Field of High Technology' (1989) 15 Monash University Law Review 219

Tate M, 'Amazon's new Alexa Update Means It Can Bring You Beer in Two Hours' (*ShortList*, 21 March 2017) <www.shortlist.com/tech/gadgets/you-can-now-tell-amazons-alexa-to-bring-you-a-beer-amazon-echo/18775> accessed 18 December 2018

Telsyte, 'Smart Speakers Help Send Australian IoT@Home Market Skyward' (*Announcements*, 15 May 2018) <www.telsyte.com.au/announcements/2018/5/15/smart-speakers-help-send-australian-iothome-market-skyward> accessed 19 June 2018

Thaler RH and Sunstein CR, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale UP 2008)

Thampapillai D, *Contract Law: Text and Cases* (2dn edn, LexisNexis Butterworths 2016)

The Innovative House, 'SmartHydro' <www.ihouse.com.br/caracteristicas-da-smarthydro.php> accessed 27 August 2018

Therapeutic Goods Administration, 'ECRI Lists Ransomware as 2018 Top Hazard' (2018) 6 Medical Devices Safety Update 2

Thierer A, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation' (2015) 21 Richmond Journal of Law & Technology 6

—— *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (revised and expanded edn, Mercatus Center at George Mason University 2016)

Tobin A, 'HUD Sues Facebook Over Housing Discrimination and Says the Company's Algorithms Have Made the Problem Worse' (*ProPublic*, 28

March 2019) <www.propublica.org/article/hud-sues-facebook-housing-discrimination-advertising-algorithms> accessed 5 April 2019

Toffler A, *The Third Wave* (Morrow 1980)

Tolentino M, 'Most Influential Countries for the Internet of Things' (*siliconANGLE*, 21 March 2014) <http://siliconangle.com/blog/2014/03/21/most-influential-countries-for-the-internet-of-things/> accessed 2 June 2014

Townsend AM, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (WW Norton & Co 2013)

Trakman LE, 'The Boundaries of Contract Law in Cyberspace' (2008) 38 Public Contract Law Journal 187

TSHX, 'Intelligent Lighting & Blinds' <www.tshx.com.au/light-blinds-automation> accessed 25 August 2018

Turban E and others, *Electronic Commerce 2012: A Managerial and Social Networks Perspective* (Global Edn, Pearson Education 2012)

Turban E and others, *Electronic Commerce: A Managerial and Social Networks Perspective* (8th Edn, Springer 2015)

Uber, 'What is Surge?' <https://help.uber.com/h/e9375d5e-917b-4bc5-8142-23b89a440eec> accessed 9 September 2018

Ubicomp, 'Ubicomp 2018' <http://ubicomp.org/ubicomp2018/> accessed 9 September 2018

Uckelmann D, Harrison M and Michahelles F, 'An Architectural Approach towards the Future Internet of Things' in Uckelmann D, Harrison M and Michahelles F (eds), *Architecting the Internet of Things* (Springer 2011)

United Kingdom, Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the Cyber Security of Consumer Internet of Things* (Report, 7 March 2018)

United Kingdom, Information Commissioner's Office, 'Actions We've Taken' <https://ico.org.uk/action-weve-taken/enforcement/> accessed 24 April 2018

United States, Commodity Futures Trading Commission and US Securities and Exchange Commission, *Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues* (30 September 2010)

United States, Copyright Office, *Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works: Second Round of Comments, Proposed Class 21: Vehicle Software – Diagnosis, Repair, or Modification*

United States, Department of Commerce, National Telecommunications and Information Administration, *Green Paper: Fostering the Advancement of the Internet of Things* (2017)

United States, Department of Defense, 'Secretary Rumsfeld and General Myers' (DoD News Briefing, 12 February 2002) <http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=2636> accessed 14 March 2017

United States, Department of Energy, Office of Electricity Delivery and Energy Reliability, 'Smartgrid.gov' <www.smartgrid.gov> accessed 9 September 2018

United States, Department of Justice, 'Cybersecurity Unit' <www.justice.gov/criminal-ccips/cybersecurity-unit> accessed 23 August 2018

United States, White House, 'The Framework for Global Electronic Commerce: Read the Framework' (July 1997) <https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html> accessed 24 April 2019

University of Oxford, Faculty of Law, *OSCOLA: The Oxford University Standard for Citation of Legal Authorities*(4th edn, Hart Publishing) <www.law.ox.ac.uk/sites/files/oxlaw/oscola_4th_edn_hart_2012.pdf> accessed 30 June 2018

Urquhart L, Lodge T and Crabtree A, 'Demonstrably Doing Accountability in the Internet of Things' (2019) 27 International Journal of Law & Information Technology 1

Uteck A, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (PhD thesis, University of Ottawa 2013)

van Boom W and Ogus A, 'Introducing, Defining and Balancing "Autonomy v Paternalism"' (2010) 3 Erasmus Law Review 1

Van Hoecke M and Warrington M, 'Legal Cultures, Legal Paradigms and Legal Doctrine: Towards a New Model for Comparative Law' (1998) 47 ICLQ 495

van Kranenburg R and others, 'The Internet of Things' (1st Berlin Symposium on Internet and Society, October 25–27, 2011)

Vargas P, 'Vignette Question' in Lavrakas PJ (ed), *Encyclopedia of Survey Research Methods* (Sage Publications 2011)

Vladeck DC, 'Machines Without Principals: Liability Rules and Artificial Intelligence' (2014) 89 Washington Law Review 117

Vout P, 'Unconscionability and Good Faith in Business Transactions' (National and Commercial Law Seminar Series, Federal Court of Australia, Monash University Faculty of Law, Commercial Bar Association of Victoria)

Vulkanovski A, 'Home, Tweet Home': Implications of the Connected Home, Human and Habitat on Australian Consumers (Australian Communications Consumer Action Network, February 2016)

Wachter S, Mittelstadt B and Floridi L, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76

Wagner, B, 'Ethics as an Escape from Regulation: From ethics-washing to ethics-shopping?', in Emre Bayamlioglu and others (eds), *Being Profiled: Cogitas Ergo Sum* (Amsterdam University Press, 2018).

Walker Smith B, 'Proximity-Driven Liability' (2013–14) 102 Georgetown Law Journal 1777

Walsh T, *It's Alive! Artificial Intelligence from the Logic Piano to Killer Robots* (La Trobe UP 2017)

Want R, 'An Introduction to Ubiquitous Computing' in Krumm J (ed) *Ubiquitous Computing Fundamentals* (Chapman & Hall/CRC 2009)

Waymo <https://waymo.com/> accessed 23 August 2018

We-Vibe <https://we-vibe.com/> accessed 1 January 2018

Webb T and Dayal S, 'Medical Devices and the IoT: Regulatory Perspectives on Cybersecurity Risks in Health Care' (2018) Internet Law Bulletin 138

Weber RH and Weber R, *Internet of Things: Legal Perspectives* (Springer 2010)

Weiser M and Brown JS, 'The Coming Age of Calm Technology' in Denning PJ and Metcalfe R (eds), *Beyond Calculation: The Next 50 Years of Computing* (Springer 1997)

Weiser M, 'The Computer for the 21st Century' (1991) Scientific American 94

—— 'The World is Not a Desktop' (1994) Interactions 7

—— 'Ubiquitous Computing' (1996) <www.ubiq.com/hypertext/weiser/UbiHome.html> accessed 10 February 2018

Wendehorst C, 'Consumer Contracts and the Internet of Things' in Schulze R and Staudenmayer D (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Hart Publishing 2016)

Werbach K, 'Sensors and Sensibilities' (2007) 28 Cardozo Law Review 2321

Westrum R, *Technologies and Society: The Shaping of People and Things* (Wadsworth 1990)

White S, 'Standards and Standard-Setting in Companion Animal Protection' (2016) 38 Sydney Law Review 463

Wilkenfeld G, 'Smart Meters, Displays and Appliances' (*Australian Government*, 2013) <www.yourhome.gov.au/energy/smart-meters-displays-and-appliances> accessed 20 August 2018

Wind J and Mahajan V, 'Digital Marketing' (2002) 1 SYMPHONYA Emerging Issues in Management 43

—— 'Convergence Marketing' (2002) 16 Journal of Interactive Marketing 64

Wong E and Lawrence A, 'From Shrink to Click and Browse: Ensuring the Enforceability of Web Terms' (2004) 7 Internet Law Bulletin 61

Wood J, 'iBeacon: The Future of Content Marketing?' *B2B Marketing* <https://www.b2bmarketing.net/en/resources/blog/ibeacon-future-content-marketing> accessed 17 February 2014

Workstream 3: Data Use AaP, *Good Data Practice: A Guide for Business to Consumer Internet of Things Services for Australia, V1.0* (November 2017)

Wright D and others (eds), *Safeguards in a World of Ambient Intelligence*, vol 1 (The International Library of Ethics, Law and Technology, Springer 2008)

Wu T, 'Agency Threats' (2011) 60 Duke Law Journal 1841

Wu Y, Kosinski M and Stillwell D, 'Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans' (Proceedings of the National Academy of Sciences of the USA, 27 January 2015)

Yeung K, 'Are Human Biomedical Interventions Legitimate Regulatory Policy Instruments?' in Brownsword R and others (eds), *Oxford Handbook of Law, Regulation and Technology* (OUP 2017)

Yu A and others, *Response to Issues Paper on Human Rights and Technology* (2018)

Yuvaraj J, 'How About Me? The Scope of Personal Information under the Australian Privacy Act 1988' (2018) 34 Computer Law and Security Review 47

Zammit JP and Savio MA, 'Tort Liability for High Risk Computer Software' (1987) 23 PLI/Pat 373

Zanero S, 'Cyber-Physical Systems' (2017) 50 Computer 14

Zarsky TZ, 'Privacy and Manipulation in the Digital Age' (2019) 20 Theoretical Inquiries in Law 157

Zelkha E and Epstein B, 'From Devices to "Ambient Intelligence": The Transformation of Consumer Electronics' (Presentation slides circulated internally within Royal Philips Electronics, 24 June 1998) <www.epstein.org/brian/ambient_intelligence.htm>

Zellner K, 'The Internet of Things and the Law' (ABC Radio National, *The Law Report*, 6 March 2018)

Zetter K, 'Medical Devices That Are Vulnerable to Life-Threatening Hacks' (*Wired*, 24 November 2015) <www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x> accessed 3 May 2016

Zhou C and others, 'Industrial Internet of Things (IIoT) Applications in Underground Coal Mines' (2017) 69 Mining Engineering 50

Zittrain J, *The Future of the Internet and How to Stop It* (Yale UP 2008)

Zorzi M and others, 'From Today's INTRAnet of Things to a Future INTERnet of Things: A Wireless- and Mobility-Related View' (2010) 17 Wireless Communications, IEEE 44

Zuboff S, 'Big other: surveillance capitalism and the prospects of an information civilization' (2015) 30 Journal of Information Technology 75

Zweigert K and Kotz H, *Introduction to Comparative Law* (3rd revised edn, Clarendon Press 1998)

Zwerdling D, 'Your Home is Your … Snitch?' (*The Marshall Project*, 24 May 2018) <www.themarshallproject.org/2018/05/24/your-home-is-your-snitch> accessed 11 September 2018