University of New South Wales Law Research Series

Emerging Information Technologies: Challenges for Consumers

KAYLEEN MANWARING

[2017] *UNSWLRS* 25

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Title: Emerging information technologies: challenges for consumers

Author: Kayleen Manwaring, School of Taxation & Business Law, UNSW Business, UNSW Sydney

Abstract

A 'third wave' of computing is emerging, encompassing technologies that have been called many names, including ubiquitous and pervasive computing, ambient intelligence, the Internet of Things and eObjects. This third wave will bring about significant socio-technical change, especially in the lives of consumers. With this change comes the possibility of a disconnection between consumer protection law and the new things, activities and relationships enabled by the third wave. This article analyses the attributes of these technologies, and identifies where consumers may face challenges relating to acquisition and interaction. These challenges are appraised in the light of common consumer protection principles, to identify whether likely detrimental outcomes for consumers may conflict with these principles. This article provides a basis for consumer protection lawyers in Commonwealth jurisdictions to examine whether or not their current consumer protection legislation can adequately provide appropriate consumer protection in the face of the third wave.

KEYWORDS: Internet law; eObjects; consumer protection; Internet of Things; ubiquitous computing; ambient intelligence

A. Introduction

A 'third wave' of computing is emerging, encompassing devices and infrastructures that depart from conventional forms of distributed computing, embedding miniaturised and networked computers in everyday objects, such as cars, fridges, people and animals. This third wave has the potential to bring about significant socio-technical change, especially in the lives of consumers who acquire and/or interact with these technologies. With this change comes the possibility of disconnections between current consumer protection law and the new things, activities and relationships enabled by the third wave.[1]

In most jurisdictions, there is limited legislative or judicial analysis of the possibility of such disconnections, although recently some industry and consumer groups have begun preliminary policy evaluations.[2] As these technologies become more prevalent, legislatures, policymakers and judges will all need to consider whether existing law can adequately regulate the new things, activities and relationships now emerging. This paper is intended to provide a basis for lawyers in different jurisdictions to examine whether their current laws provide acceptable levels of consumer protection in the face of the third wave.

Third wave technologies have been called many names, such as ubiquitous and pervasive computing, ambient intelligence, and the Internet of Things. The inconsistency and intersecting nature of terminology usage over country, time and research institution makes the use of all or any one of these terms problematic.[3] To

[1] Kayleen Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2016) 21 Deakin Law Review (forthcoming); 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.

[2] Eg Alexander Vulkanovski, *"Home, Tweet Home": Implications of the Connected Home, Human and Habitat on Australian Consumers* (Australian Communications Consumer Action Network, Sydney, February 2016); Geof Heydon and Frank Zeichner, *Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act* (Industry Report, Communications Alliance Ltd, October 2015); 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; 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).

[3] Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research into Networked eObjects' (2015) 31 Computer Law & Security Review 586. As an example of these problems, in 2015 one researcher identified over 60 different definitions of the term 'Internet of Things'. 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.

avoid these problems, in this paper I adopt the approach proposed by Manwaring and Clarke[4] in 2015, and use their term 'eObjects' (enhanced objects). 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.[5]

Such a shorthand definition, while helpful, cannot however be complete, considering the variety and complexity of the technologies. Manwaring and Clarke also proposed a framework of core and common attributes, and interactions, to give a more complete view of the technologies. A summary of this framework is given in the Appendix.

Most of the discussion of eObjects to date has concentrated on the inadequacy of existing privacy and data protection laws.[6] These are undeniably important to consumers, but do not tell the whole story. Until recently, only a small amount of literature raised misgivings about other effects on consumers and their contracts with suppliers.[7] From late 2015, however, greater concern began emerging in some government departments and consumer groups about these types of challenges for consumers acquiring and interacting with eObjects.[8] These challenges can arise not only in relation to the core and common attributes of eObjects but in the contractual arrangements used to supply them to consumers.

Part B of this paper describes a set of consumer protection principles (**CPPs**) derived from the recently revised *United Nations Guidelines for Consumer Protection* (**2015 Guidelines**).[9] Part C uses the eObjects attributes/interaction framework summarised

---

[4] Manwaring and Clarke, 'Surfing the Third Wave of Computing' (n 3).
[5] Manwaring and Clarke, 'Surfing the Third Wave of Computing' (n 3) 599.
[6] Eg Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent' (2014) 93 Texas Law Review 85; Adam D Thierer, 'The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation' (2015) 21 Richmond Journal of Law & Technology; Anne Uteck, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (PhD thesis, University of Ottawa 2013); James Ridge, 'What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive' (2007–2008) 49 South Texas Law Review.
[7] Joshua Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (2012) 27 Berkeley Technology Law Journal 55; Scott R Peppet, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (2012) 59 UCLA Law Review 676; Peppet, 'Regulating the Internet of Things' (n 6); Nancy S Kim, 'Two Alternate Visions of Contract Law in 2025' (2014) 52 Duquesne Law Review; 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; Ryan Calo, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review 995.
[8] Eg Coll and Simpson, *Connection and Protection in the Digital Age* (n 2); Vulkanovski, *"Home, Tweet Home"* (n 2).
[9] United Nations General Assembly, *United Nations Guidelines for Consumer Protection* (2015).

in the Appendix to identify the challenges consumers may face when entering into a contract relating to eObjects (these attributes are identified by *italics*). Part C proceeds to identify whether likely detrimental outcomes for consumers faced with these challenges may conflict with the CPPs. This provides a basis for Commonwealth scholars and policymakers to assess whether their consumer protection laws are adequate to address the supply to and use of eObjects by consumers. Part D concludes the article by highlighting some of the most important legal areas that should be investigated in individual jurisdictions.

B. Consumer protection principles

The 2015 Guidelines were adopted by the UN General Assembly in December 2015, comprising a revised version of Guidelines originally adopted in 1985 (**Old Guidelines**).[10] The 2015 Guidelines contain a set of principles intended to describe 'the main characteristics of effective consumer protection legislation, enforcement institutions and redress systems'.[11] These consumer protection principles can be summarised as:

Section of 2015 Guidelines	Description	Abbreviation
III.5(a), V.E	Consumers should have access to essential goods and services	**Essentials**
III.5(b), IV.11(a)	Consumers who are vulnerable or disadvantaged should be protected	**Disadvantage**
III.5(c), V.B, V.D	Consumers should be protected against threats to health and safety	**Safety**
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**

[10] 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.
[11] United Nations General Assembly, *United Nations Guidelines for Consumer Protection*, Preface, 3.

III.5(d), V.C	Businesses should supply goods and services which are durable, reliable and fit for purpose	**Quality**
III.5(e), IV.11(c)	Consumers should be given access to sufficient information to make informed individual choices	**Information**
III.5(f), V.G	Consumers should be given access to education programmes	**Education**
III.5(g), V.F	Effective dispute resolution and redress should be provided to consumers	**Redress**
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**
III.5(i), V.H	Sustainable consumption by consumers should be promoted	**Sustainability**
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**

The most significant changes introduced by the 2015 Guidelines included:

- the inclusion of the CPP of Parity for electronic commerce;
- a consumer right to Privacy; and
- protection against Disadvantage.

The CPPs contained in the Old Guidelines have generally been adopted, in whole or in part, by UN member states, including Commonwealth countries.[12] Of course, the consumer protection laws in each Commonwealth jurisdiction differ in their detail, and there has been little time for UN member states to revise their consumer protection legislation to ensure compliance with the 2015 Guidelines. However, the history of broad adoption of the UN Guidelines means the CPPs provide a useful preliminary basis on which to assess the adequacy of a Commonwealth country's

[12] United Nations Conference on Trade and Development, *Implementation Report on the United Nations Guidelines on Consumer Protection (1985–2013)*; Consumers International, *The State of Consumer Protection Around the World 2013*.

consumer protection law in the face of socio-technical change brought about by eObjects.

C. Challenges for consumers

So what aspects of eObjects might pose challenges for consumers that may conflict with these CPPs? This paper argues that consumers face significant challenges due to the following features of eObjects:

1. eObjects are **imperfect** (see C.1);
2. eObjects can be **controlled** and **modified** remotely by suppliers and others in the provider network[13] (see C.2);
3. eObjects have the capacity to **manipulate** or **impede consumer choice** (see C.3);
4. eObjects have a significant **post-supply value** to suppliers and other related goods and services providers (see C.4); and
5. eObjects are **complex** (see C.5).

1. eObjects are imperfect

Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability[14] to ensure eObjects are reliable in their operation, and this gives rise to particular challenges for consumers. Possible harms to consumers faced with the challenges described in this section raise potential conflicts with the CPPs of **Quality** and **Safety**. Some also raise conflicts with other CPPs, as set out below.

a. Risks of failure

Vulnerability is an important attribute of consumer eObjects. In 2001, in the early days of eObjects, Satyanarayanan argued that eObjects are more prone than conventional

[13] I use this term 'provider network' in preference to the commonly used 'supply chain', as the latter term implies linear progressive connections. In an eObject context, the provider connections are much more likely to be distributed or weblike in nature rather than linear.
[14] Peppet, 'Regulating the Internet of Things' (n 6) 135–36.

connected computers to physical interference and remote attacks.[15] A deluge of reports in the last few years has supported this view. Security vulnerabilities have been identified in: fitness trackers;[16] medical eObjects such as insulin pumps, heart defibrillators and CT scans;[17] domestic appliances such as Internet-connected kettles,[18] baby monitors,[19] childrens' toys[20] and location trackers;[21] as well as guns[22] and cars,[23] just to name a few.

The increased risk of security exploits is due to the existence of particular security vulnerabilities in the eObjects themselves and the systems to which these are connected, such as inadequate encryption, weak passwords, lack of account lock out, poor authentication, authorisation and updating practices, and the lack of physical safeguards.[24] The nature of many manufacturers as consumer goods specialists rather than ICT specialists, the smaller size of many devices, and design flaws prohibiting

[15] Mahadev Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (1996) *Principles of Distributed Computing: Proceedings of the Fifteenth Annual ACM Symposium* 1.
[16] Eg Fitbit. See Mahmudur Rahman, Bogdan Carbunar and Madhusudan Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) arXiv:13045672 [csCR] and Mario Ballano Barcena, Candid Wueest and Hon Lau, *How Safe is Your Quantified Self?* (Symantec Security Response Report, 11 August 2014).
[17] Anthony M Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (W. W. Norton & Company 2013) 269. Other healthcare eObjects with identified security concerns include drug infusion pumps, X-ray systems and blood refrigeration units. See also Kim Zetter, 'Medical Devices That are Vulnerable to Life-threatening Hacks' Wiredcom < http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x > accessed 3 May 2016.
[18] 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.
[19] Kashmir Hill, 'Crib Cams: Watch Out New Parents – Internet-connected Baby Monitors are Easy to Hack' Fusionnet (3 September 2015) < http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/ > accessed 1 March 2015.
[20] Security Ledger, 'Update: Hello Barbie Fails Another Security Test' securityledgercom (4 December 2015) < https://securityledger.com/2015/12/hello-barbie-fails-another-security-test/ > accessed 17 December 2015.
[21] Lorenzo Franceschi-Bicchierai, 'A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them' (2 February 2016) < http://motherboard.vice.com/read/a-gps-tracker-for-kids-had-a-bug-that-wouldlet-hackers-stalk-them > accessed 20 June 2016.
[22] Andy Greenberg and Kim Zetter, 'How the Internet of Things Got Hacked' Wired (28 December 2015) < https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/ > accessed 20 June 2016.
[23] Andy Greenberg, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' Wired (21 July 2015) < http://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, 'Bits Blog: Disruptions: As New Targets for Hackers, Your Car and Your House' *The New York Times* (11 August 2013) < http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0 > accessed 2 Feb 2017.
[24] Open Web Application Security Project, 'OWASP Internet of Things Project' (2014) < https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29 > accessed 12 January 2017.

software patches have all been attributed as reasons why security problems arise so commonly in eObjects.[25]

Security attacks resulting from these vulnerabilities include unauthorised remote operation of the eObject ('hacking') and/or the delivery of malware. When these attacks occur, sensitive data might be disclosed or modified, or the eObject could be used to attack other eObjects or conventional computers. For example, in September 2016, the website of the security journalist Brian Krebs was targeted by a distributed denial of service attack delivered primarily through eObjects.[26] Of course, such attacks are also delivered using conventional computers. What is more particular to eObjects is physical harm that might arise to the eObject, surrounding objects and/or other living things.[27]

The potential for physical harm is likely to come to prominence when the attribute of *vulnerability* interacts with the attribute of *mobility* and/or *active capacity*. Desktop computers cannot be thrown across a room by a hacker. But in recent years, security researchers have managed to find ways to control connected cars' locks, brakes, steering and transmission remotely.[28] Internet-connected kettles have been exposed as significant security threats.[29] Therefore, the potential for anonymous and distant hackers to cause injury by wresting control from drivers of heavy objects travelling at speed, or to find an entry point into a smart home where connected sprinklers could be turned off and hotplates turned on, are just a couple of examples where consumer eObjects could be used to cause physical harm. With the rise of ransomware, which has already been used to breach medical eObjects,[30] there exists a financial incentive to threaten such harm.

---

[25] Peppet, 'Regulating the Internet of Things' (n 6), 135–36; Bruce Schneier, 'The Internet of Things is Wildly Insecure – and Often Unpatchable' Wired (1 June 2014) < http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/ > accessed 17 December 2015.
[26] Brian Krebs, 'KrebsOnSecurity Hit With Record DDoS' (2016) < https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/ > accessed 24 October 2016.
[27] Cloud Security Alliance Mobile Working Group, *Security Guidance for Early Adopters of the Internet of Things (IoT)* (April 2015).
[28] See n 23.
[29] Cimpanu, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks Across London' (n 18).
[30] Heather Landi, 'Report: Ransomware Attacks on IoT Medical Devices Will Likely Increase' Healthcare Informatics (29 November 2016) < http://www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware > accessed 13 January 2017.

Many, if not most, eObjects or their associated systems have an attribute of *volatility*: that is, limited or intermittent access to resources needed to operate, particularly network connections, energy sources and processing power.[31] This constraint is a particular challenge for users of *mobile* eObjects, where the size, weight and form of the eObject dominate design decisions,[32] often at the expense of resource allocation. For example, mobile eObjects currently need to be designed to minimise power usage, which can negatively affect power and speed of processing. For simple applications, this constraint may matter little: a delay in email is rarely life-threatening. But when we consider healthcare eObjects, such as insulin pumps and pacemakers, the draining of a power source or the loss of connectivity leading to loss of control can cause serious harm, even death.

b. Risky decision-making: inaccuracy and autonomy

All eObjects have the capacity to *collect*, *handle* and *communicate data*.[33] 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. For example, questions have already been raised about the accuracy of accelerometers[34] and sleep trackers.[35]

Consumers, the provider network and others who rely on accurate data (for example, users and receivers of insulin injections) are of course at the risk of physical or other harm if such data is inaccurate.[36] This is particularly the case where the eObject has *autonomous* decision-making capabilities: decisions may be made for the user without adequate notification and/or capacity for manual override. Even before eObjects were produced, risks have been identified arising from autonomous objects with *active capacity*. For example, in the mid-80s, two people died and a number of others were

---

[31] George F Coulouris and others, *Distributed Systems: Concepts and Design* (Addison-Wesley 2012) 817.
[32] Mahadev Satyanarayanan, 'Fundamental Challenges in Mobile Computing' (1996) *Principles of Distributed Computing: Proceedings of the Fifteenth Annual ACM Symposium* 1.
[33] Manwaring and Clarke, 'Surfing the Third Wave of Computing' (n 3).
[34] 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.
[35] HE Montgomery-Downs, SP Insana and JA Bond, 'Movement Toward a Novel Activity Monitoring Device' (2012) 16 Sleep Breath 913.
[36] W Kuan Hon, Christopher Millard and Jatinder Singh, *Twenty Legal Considerations for Clouds of Things* (4 January 2016) Queen Mary School of Law Legal Studies Research Paper 216/2016 < http://dx.doi.org/10.2139/ssrn.2716966 >

injured when computerised radiotherapy machines in a series of hospitals administered massive overdoses of radiation to patients, partially due to an incorrect zero value in a failsafe counter.[37] Although the risks are not new, a significant increase in the prevalence of autonomous eObjects has the potential to increase the likelihood of such incidents occurring, particularly when such objects are also *vulnerable* to security breaches.

Even when data is accurate, eObjects with some autonomous decision-making capability are also risky. Decision-making algorithms could be programmed to result in outcomes not desired by the user. Consumers rarely have transparency as to the content of such algorithms, and most are not equipped to understand them even if they did. Additionally, there are some machine learning technologies in development where it is anticipated that decision-making will not be completely deterministic, meaning that even the original programmers may not be able to predict the results.[38]

An eObject's decision-making capabilities could also cause economic harm, for example if it institutes a contract for purchase not desired by a consumer. For example, the automatic reordering function made available by products like Amazon Dash Buttons[39] may cause problems: who is liable to pay if and when 1000 cartons of washing detergent are ordered instead of one, due to a failure in the eObject?

In addition to issues around **Safety** and **Quality**, there is a risk that the provider network will not provide sufficient **Information**. The **Redress** CPP may also be compromised, as autonomous decision-making 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?

c. Management of risk

All eObjects contain hardware, software and a physical object (which may be a living thing). Very many eObjects also constitute what Helberger calls a 'product-service

[37] NG Leveson and CS Turner, 'An Investigation of the Therac-25 Accidents' (1993) 26 Computer 18, 34.
[38] Jenna Burrell, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) Big Data & Society 1, 3–5.
[39] < https://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011 >.

package',[40] where services are provided along with the object. All of these elements of an eObject may have been provided by different entities, such as the manufacturer of the object, the programmers of the embedded software, the providers of cloud data storage and processing services, as well as other actors, depending on the complexity of the eObject and the system in which it participates.[41]

The management of risk is complicated in regard to eObjects because of the nature of many eObjects as product-service packages, and further so when there are a number of players in the provider network. There are three main challenges:

- Proactive management of risk: what are the provider network obligations in relation to monitoring and updating of software?[42]
- When things go wrong: who will be responsible for fixing problems with the eObject?[43]
- What limitations will entities in the provider network attempt to place on their obligations regarding risk management?

Considering the risks outlined above, these are important things for the consumer to know before they enter into a contract. Say a consumer lives in a house with a smart lock system. She has just separated from her partner, who until the separation lived at the same address. Due to threats of violence, she has changed the password on the locks, and has taken out an apprehended violence order against her ex-partner. Hackers discover a vulnerability in the system, and publish details on the World Wide Web on how to exploit it.

The consumer would be concerned with the following questions:

- Is any security monitoring being done by the provider network?
- Will the consumer be notified if there is a vulnerability? And if so, when?
- Who is responsible for supplying security patches and when will they be available?

[40] 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) 6 (page no is based on SSRN version at < http://ssrn.com/abstract=2728717 >).
[41] See eg 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 for a detailed description of the large number of product and service providers that can be involved in provision and support of an eObject.
[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) 194–95.
[43] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 41) 195–96.

- 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 supplier liability for damage caused due to the failure of the smart lock? Does it cover repair, damage to property, personal harm?
- If the ex-partner is the contracting party for the locking system, what redress does the consumer have?
- What happens if the security provider goes out of business?

Consumer judgment on the adequacy of answers to these questions may well be essential when choosing between competing products. In cases where information is not readily available, or is unintelligible or imprecise, this will lead to a conflict with the CPP of **Information**. In addition, if suppliers are allowed to drastically limit their liability without some form of core responsibility, then this would come into conflict with the CPPs of **Safety**, **Quality** and **Redress.**

2. eObjects can be controlled and modified remotely by the provider network

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 associated services may be designed to allow entities in the provider network to control or modify the eObject, the data held within it, and/or the services supplied along with the eObject, potentially without the consumer even realising what has been done and certainly without the means to prevent it. This can raise issues in ensuring the CPPs of **Fairness** and **Safety** are not compromised.

Most physical consumer goods are only subject to change imposed by time or by parties controlled by the customer. However, the potential for remote modification in eObjects means that members of the provider network may be able to:

- disable temporarily or permanently all or part of an eObject's functionality;
- program the eObject to work differently;
- 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.[44]

A connected eObject can be remotely disabled from working, for example where a purchase instalment or a related service fee has not been paid. Starter interrupt devices (installed in approximately 2 million cars in the US by late 2014) allow lenders or their agents to remotely disable a vehicle using their mobile phone, which they are contractually entitled to do when owners are late on car repayments.[45] This ability to remotely disable an eObject gives the provider network powerful new private enforcement capabilities, leading to some unique situations. For example, the remote triggering of a starter interrupt device reportedly prevented a mother from taking her asthmatic child to the hospital, and another woman was forced off the road when her car powered down, allegedly due to the use of an interrupt device by her lender.[46]

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 release, after Revolv was acquired by a company that refused to support the product.[47] This 'bricking' of eObjects can be effected in other ways, such as in the case where a supplier issues an upgrade to firmware or other software that reduces the speed of the eObject's data-handling

[44] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 41) 200–02; Bryant Walker Smith, 'Proximity-Driven Liability' (2013–2014) 102 Georgetown Law Journal 1777.
[45] Michael Corkery and Jessica Silver-Greenberg, 'Miss a Payment? Good Luck Moving That Car' *The New York Times* (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 Feb 2017
[46] Corkery and Silver-Greenberg, 'Miss a Payment? Good Luck Moving That Car' (n 44).
[47] Woodrow Hartzog and Evan Selinger, 'The Internet of Heirlooms and Disposable Things' (2016) 17 North Carolina Journal of Law & Technology 581, 584.

capabilities to a level that makes the hardware unusable.[48] Or a service provider may go into liquidation or simply decide to discontinue a service, such as cloud data storage and processing. This can make the eObject worthless to the consumer, for example where the eObject was designed to communicate only with a proprietary service. In the end, a consumer may have no choice but to buy a new device with upgraded hardware, or to pay a premium price for an upgraded service. Other than the impact on individual consumers, this contribution to the world's e-waste problems could also breach the CPP of **Sustainability**.

Digital content that is resident in or accessed through eObjects may well be blocked to protect rights holders; such as when there is no record of a user holding a licence to that content,[49] but also in cases where the consumer has not been involved in a breach of contract or any wrongdoing. For example, in 2009, Amazon remotely deleted copies of the novel *1984* from customers' e-book readers when Amazon discovered it had been made available in its store by an unlicensed vendor.[50]

Some types of remote disablement may produce the same result as a court order. However, the challenge for consumers subsists in the one-sided nature of the remedy, as well as the immediacy and the inflexibility of such supplier reactions. Safeguards brought about by the engagement in a formal dispute resolution process, overseen by a neutral party, the court, will no longer apply to protect the consumer except well after the detriment has had an impact.[51]

The situations outlined above indicate a clear conflict with the CPP of **Quality**, and in some cases, **Safety** and **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, by a deliberate or inadvertent act by the supplier or someone else in the provider network, that the case becomes otherwise. Suppliers' ability to act in this way, often supported by non-negotiable contractual terms explicitly granting the right to such modifications, could also conflict with the CPP of **Fairness**.

---

[48] See eg user comments in Samuel Gibbs, 'iOS9 Making Your iPhone Slow? You're Not Alone' *The Guardian* (24 September 2015) < https://www.theguardian.com/technology/2015/sep/24/iphone-slow-ios-9-update-iphone-4s-iphone-5-iphone-5s > accessed 12 January 2017.

[49] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 42) 201–02.

[50] Brad Stone, 'Amazon Erases Orwell Books From Kindle' *The New York Times* (18 July 2009) < http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html > accessed 18 May 2016.

[51] Coll and Simpson, *Connection and Protection in the Digital Age* (n 2) 35–36.

3. eObjects have the capacity to manipulate or impede consumer choice

Some attributes of and interactions involving eObjects can remove or impede consumers' freedom of choice, and detrimental effects on consumers arising from this limitation of choice are most likely to compromise the CPP of **Fairness**. Some behaviours may also be incompatible with the CPPs of **Disadvantage** and **Information**.

a. Digital market manipulation

Evidence presented to a recent US enquiry asserted that existing smartphone sensors can currently be used to infer:

> a user's mood; stress levels; personality type; bipolar disorder; demographics (eg gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.[52]

This type of information can be very valuable to a marketer attempting to persuade consumers to buy their products. In fact, a number of attributes present in eObjects are helpful to such a marketer, particularly when viewed in conjunction with the development of sophisticated data-processing techniques.

Many eObjects are *mobile*, and even for those that are embedded rather than mobile, the mobility of people interacting with the embedded object can increase the amount and variety of data collected, especially considering the increasing *prevalence* of eObjects. The value of *geo-locational* and *data-collection* technologies in marketing has been enhanced by the *use pattern* of eObjects, as they are likely to be 'personal'; that is, intimately associated with an individual. This personal use pattern greatly enhances both the value of the geo-locational functionality and the utility of the data gathered and communicated by the eObject.

Data utility is also increased by the *adaptability* attribute (also known as 'context-awareness'). Adaptable eObjects identify in real time some part of user context, and vary their responses accordingly. As the use of eObjects becomes more widespread,

[52] Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, 2015).

this increases the likelihood that a greater quantity of data – and data that is more intimate and personalised in quality – can and will be collected and processed. Inferences potentially derived from all of this data can be used for purposes that the owner of the eObject might find beneficial: for example, better targeting of advertising. However, there are also less beneficial uses. Digitisation of commerce generally (mediated through both conventional desktop ecommerce and eObjects) may give firms with large marketing budgets an enhanced ability not only to target consumer preferences but to exploit consumers' cognitive biases and individual vulnerabilities.[53] For example, advertisers may filter the available information; they may target consumers at the time when their willpower is lowest; or they may craft their advertisements to act upon known purchasing triggers of particular individuals, for example, feelings of guilt or obligation, or concerns about missing out, or a desire to emulate friends or celebrities. Calo has dubbed this practice 'digital market manipulation'.[54]

Currently, most examples of digital market manipulation have been identified in conventional ecommerce.[55] However, the use of eObjects in these practices is increasing. Beacon implementations, such as Apple's iBeacon, combine precise geo-location and context data (such as proximity, preferences, buying history and time of day) to target marketing communications. These implementations use indoor positioning devices and low-power sensors[56] to track subscribers' mobile phone signals. For example, when a person's phone is located close to the menswear section in a department store, this might trigger an SMS to that person offering a discount on ties. Although the use of beacon technology is not yet widespread, in 2016 was being used or piloted by retail, fast food, sporting, airline, real estate services, pharmacies and other business enterprises.[57]

---

[53] Calo, 'Digital Market Manipulation' (n 7); Kim, 'Two Alternate Visions of Contract Law in 2025' (n 7); Helberger, 'Profiling and Targeting Consumers in the Internet of Things – A New Challenge for Consumer Law' (n 40); James Halliday and Rebekah Lam, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (2016) 34 Communications Law Bulletin 4.

[54] Calo, 'Digital Market Manipulation' (n 7).

[55] Calo, 'Digital Market Manipulation' (n 7).

[56] iBeacon uses the Bluetooth Low Energy communications standard, but other beacon technologies use both Bluetooth and Wi-Fi (eg Motorola Solutions and Datzing).

[57] Woolworths Ltd (major supermarket chain), Homepass (real estate services), John Lewis (department store). See < http://localz.com/customers/ >. Also Macy's, McDonalds, Major League Baseball, Walgreens, Virgin Atlantic,

So why does this matter? Consumers have always been on the receiving end of persuasive tactics from advertisers. Data collected by eObjects will arguably provide significant advantages to marketers in accuracy, scope, scale and effectiveness.[58] The impact of scale in particular may be amplified by the implementation of software (eg Silverpush) that allows tracking across different consumer devices, particularly if done without the knowledge of the consumer.[59] The key question is 'at which point 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'.[60]

It is clear that some forms of digital market manipulation have the potential to conflict with the CPPs of **Disadvantage** and **Fairness**. However, what is unclear is where the line should be drawn. Generally, society accepts that a marketer's job is to convince a consumer to do something: but it is unclear when this type of behaviour would cross over from 'normal' marketing practice into something that is considered to be 'unfair' persuasion.[61] Should those with particular 'vulnerability profiles' be able to claim greater protection than the 'average' consumer? For example, society may look askance at a marketer who targets a habitual gambler with an offer of an extended limit on her credit card as she passes a betting shop. However, the attitude towards someone who is persuaded to buy a face cream just because his favourite celebrity's voice is used to persuade him to take advantage of a discount as he passes the cosmetics aisle in his local department store may be less sympathetic.

b. Consumer 'lock out'

The *prevalence* of eObjects may lead to a scarcity problem: non-eObject versions of consumer products may become unavailable. Consumers with legitimate concerns

---

Japan Airlines, American Airlines. Trips Reddy, '15 Companies From Airports to Retail Already Using Beacon Technology' < https://www.umbel.com/blog/mobile/15-companies-using-beacon-technology/ > accessed 10 November 2014; James Wood, 'iBeacon: the Future of Content Marketing?' B2B Marketing < http://www.b2bmarketing.net/blog/posts/2014/02/17/ibeacon-future-content-marketing > accessed 17 February 2014.

[58] Kim, 'Two Alternate Visions of Contract Law in 2025' (n 7) 312.

[59] Hartzog and Selinger, 'The Internet of Heirlooms and Disposable Things' (n 47).

[60] Helberger, 'Profiling and Targeting Consumers in the Internet of Things' (n 40).

[61] Calo, 'Digital Market Manipulation' (n 7) 1032.

about the attributes and interactions of eObjects and their disbenefits, such as in the areas of privacy and security, may find it impossible to opt out.[62]

Where *dependency* on remote resources is essential to the functionality of the eObject, this can also lock certain consumers out. Regional areas in many Commonwealth countries may not have the connectivity required for particular eObjects. If it is not profitable to make non-eObject versions, then rural and regional residents may have to function without the object at all.

This problem would appear to directly affect the CPP of **Disadvantage**, and possibly in the future, the CPP of **Essentials**.

4. eObjects have a post-supply value to suppliers

The *use pattern* of eObjects can allow significant post-supply value to be exploited; for example, in reuse or sale of the data collected by the eObject, or the long-term recoupment of contractual premiums for licences or other services provided. Many eObjects return value for suppliers additional and separate to the upfront price paid for the underlying object. For example, a fridge that is not an eObject delivers little or no post-sale value for its supplier. On the contrary, the supplier maintains a significant post-sale obligation, in the form of warranties. However, the potential for post-sale value in eObjects is significant.[63] For example, a smart fridge may deliver post-sale value to a supplier in the following ways:

- data on consumption patterns may be on-sold to supermarkets;
- ongoing service fees, such as for software maintenance and updates, or cloud data processing and handling;
- commissions for automatically ordered produce from a retail partner; and
- effective brand loyalty, once consumers looking to buy a new fridge realise if they switch brands they will need to re-enter all of their ordering data (a form of consumer 'lock in'[64]).

[62] Coll and Simpson, *Connection and Protection in the Digital Age* (n 2) 38.
[63] 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.
[64] Coll and Simpson, *Connection and Protection in the Digital Age* (n 2) 47.

a. Data

Privacy and data protection issues dominate the scholarly and popular literature on eObjects. To deal with these issues in full in relation to eObjects is outside the scope of this paper. However, some data-gathering practices by suppliers in relation to eObjects have a direct impact on consumer contracts, so they will be discussed briefly in this paper.

Consideration for eObjects in a consumer transaction is often not confined to a money price.[65] The most common form of additional consideration is a requirement of consent to the provision of personal data. Demand for data did not of course begin with eObjects, but the greater amount of data made available by eObjects, based on the *prevalence* and *mobility* of such objects, considerably increases the likelihood of suppliers requiring data as a mandatory part of the consideration for the supply contract.

The developmental tendency of the design of many eObjects towards reduced *visibility* can also affect this situation, to the detriment of the consumer. Unobtrusiveness of the data-gathering function in many eObjects can intensify existing problems around data collection, storage and redistribution. An effectively invisible eObject will not advertise the data being collected, and if that is the case, how can a person unknowingly interacting with it exercise any real choice in prohibiting or limiting the use of information gathered?

The eObject itself need not be invisible in order to cause problems, just its data-gathering function. In 2016, an Illinois consumer brought a class action against Standard Innovation (US) Corp, the manufacturer of the 'We-Vibe' vibrator. Consumers and their partners can pair the We-Vibe via Bluetooth with a smart phone 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

[65] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 42) 193–94.

customers … allowing [Standard Innovation] to link the usage information to specific customer accounts.[66]

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.[67] This is a clear breach of the new CPP of **Privacy**.

Two significant challenges for consumers arise in relation to the data demanded by suppliers as part of the supply of eObjects. These are ensuring that consumers:

i. are aware of what data is being collected, to whom it will be provided, and for what purpose ('**data awareness**'); and
ii. can take their data with them if they terminate their use of the original eObject, for example, to move to another brand ('**data portability**').

If these challenges are not met by the provider network, the concern arises that the CPP of **Information** may also be compromised. Also, mandatory data requirements, even when the consumer has been fully informed, could arguably breach the **Fairness** CPP in certain circumstances.[68]

b. Post-supply restrictions

The nature of eObjects in containing a programmable computer with data collection and handling capabilities means in every eObject some form of software will need to be provided. Other forms of eObjects, such as e-book readers and networked media players, will also contain quite a substantial amount of digital content aside from software.

Post-supply restrictions on the consumer may arise in many different ways. For example:

- consumers may be required to enter into an ongoing service contract, such as for cloud data processing and storage;

[66] Complaint, *NP v Standard Innovation (US) Corp*, Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois, para 19.
[67] Complaint, *NP v Standard Innovation (US) Corp* (n 65) para 23.
[68] Helberger, 'Profiling and Targeting Consumers in the Internet of Things' (n 40) 147–51.

- the eObject may not be 'sold' to the consumer, in terms of granting full transfer of property rights – the supply contract may be a lease or licence, imposing an obligation to return the eObject on breach or termination;[69]
- the supply may be subject to restrictive licence terms for the software or other digital content, such as those restricting copying, modification or particular types of use (included in separate agreements such as End User Licence Agreements [EULAs] or alternatively in the supply agreement itself). These terms may also effectively prevent resale of the eObject, even if property in the physical device is transferred outright; and
- the original set-up of the eObject may impose mandatory and irreversible personalisation of the eObject (such as user names, inability to delete data) that may limit its resale attractiveness.[70]

Challenges for consumers arising out of these post-supply obligations include:

- post-supply notification: consumers may not be 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 set-up;
- greater restrictions on use compared with a non-eObject version;
- 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;[71] and
- more significant penalties for breach of use restrictions, such as those contained in anti-hacking[72] and/or copyright legislation, as opposed to civil remedies for contractual breach.

These types of post-supply obligations can severely restrict a consumer's choice, not necessarily of the first purchase of the eObject, but as to third party service providers

[69] Walker Smith, 'Proximity-Driven Liability' (n 44) 1815–16; Fairfield, 'Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life' (n 7); Hon, Millard and Singh, *Twenty Legal Considerations for Clouds of Things* (n 36).
[70] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 42) 201.
[71] Although of course black markets will continue to exist unless and until software suppliers win the war on digital rights management technologies.
[72] Walker Smith, 'Proximity-Driven Liability' (n 44) 1815–16.

and the subsequent purchase of other products. These types of walled gardens may unreasonably fetter effective competition.

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 CPP of **Information**. Unreasonable restrictions on post-supply use will also compromise the CPP of **Fairness**.

5. eObjects are complex

The core attributes of an eObject mean there is no such thing as a 'simple' eObject. Even the most basic eObject is a hybrid of software, hardware and physical object, usually inseparable,[73] and many eObjects are *dependent* on additional services, such as data processing. Software and services are often supplied by more than one entity in the provider network. 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.

There are two types of complexity that give rise to challenges for consumers:

- the complexity of the technology itself; and
- the complexity of the contractual arrangements surrounding the supply of eObjects.

The nature of eObject ecosystems promotes the likelihood of numerous actors in the provider network. The existence of a complex provider network will mean the contractual arrangements and therefore liability allocation will also be complex. For example, even a simple eObject such as a thermostat could require a multitude of separate contracts dealing with hardware, software development, software licences, installation, website and app usage, payment services, connectivity provision, sale,

[73] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41) 12; Coll and Simpson, *Connection and Protection in the Digital Age* (n 2) 33.

distribution and rental.[74] These contracts may be with separate entities, some of whom have no connection (or even knowledge) of others in the provider network.[75]

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) as well as actors in the provider network.[76] For example, the Nest thermostat 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.[77] Therefore, the likelihood of conflicting terms and conditions[78] is high, as is uncertainty of their effects for consumers as well as those in the provider network.

Challenges for consumers therefore arise in meeting the CPPs of **Information** and **Redress**.

a. Making an informed choice

A consumer, when entering into a contract, requires sufficient, accurate and intelligible information on the nature, features and dependencies of the product or service the consumer is buying, in order to meet the CPP of **Information**. A supplier need only supply minimal information to fulfil this requirement when supplying a simple product. The complexity of eObjects, particularly product-service packages, will at times require somewhat more than minimal information to sufficiently inform a consumer in order for them to make a sensible purchasing decision. And mere provision of information by one supplier is insufficient – the consumer's knowledge of the alternatives on offer and her/his judgment of the price and quality differences is also required.[79]

Consumers face three main challenges to receiving adequate **Information**:

i. the type of information required (**content**);

---

[74] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[75] Hon, Millard and Singh, *Twenty Legal Considerations for Clouds of Things* (n 36) 7.
[76] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[77] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41) 9.
[78] Hon, Millard and Singh, *Twenty Legal Considerations for Clouds of Things* (n 36) 16, citing generally an earlier version of Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[79] Productivity Commission, *Review of Australia's Consumer Policy Framework* (Final Report, Canberra 2008) vol 2, 28.

ii. whether the consumer can adequately understand the information provided (**intelligibility**); and
iii. when and how the information is provided (**delivery mechanism**).

i. Content

Consumer knowledge of the functionality of the device, system or product-service package acquired is important, as is its suitability for the consumer's particular purposes. Knowledge of 'normal' functionality will usually be insufficient for a consumer's purposes, particularly when dealing with eObjects with significant *volatility* and/or *dependencies*: such eObjects will face significant limitations on functionality in particular situations, for example use in areas with weak network connectivity.[80]

Knowing exactly what the eObject does is not only important so consumers can assess whether it meets their needs. It is also important because the post-supply value of eObjects (particularly data collection) can provide an incentive to suppliers to include features that are beneficial to the supplier or others in the provider network but are a disbenefit to consumers and therefore can affect their decision on whether they wish to buy the eObject. Such functionality may well be *invisible* or unobtrusive**:** meaning an overt disclosure of this 'dark'[81] functionality may need to be formally required or otherwise consumers may remain unaware, such as in the We-Vibe example above.

Aside from functionality of the device itself, the attribute of *dependency* and the nature of eObject interactions mean specific information on interoperability will often be critical. A smart kettle that cannot connect to a particular type of home network could have consequences in terms of its innate usability and/or its ongoing usage costs. If, for example, a homeowner was not told the kettle was only usable if connected through the homeowner's mobile network (with associated higher data costs), then the bargain may well be substantially different than the consumer

[80] Wendehorst, 'Consumer Contracts and the Internet of Things' (n 42) 191–92.
[81] This term is adopted from the 'dark scenarios' terminology used in the SWAMI research project. See David Wright and others (eds), *Safeguards in a World of Ambient Intelligence*, vol 1 (The International Library of Ethics, Law and Technology, Springer 2008).

expected. Alternatively, particular systems may only allow add-in of particular brands of eObjects,[82] therefore restricting the freedom of choice for consumers.

Clear information on price is fundamental to any consumer contract. This is of course not just the upfront money price paid for the initial supply, but also 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. Consumers should also be aware of non-money considerations, such as post-supply obligations of the consumer, for example in relation to data and use restrictions.

Ascertaining payment terms may also be problematic, as may the consequences for 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.

Gaps in providing this content may compromise the CPP of **Information**.

ii. Intelligibility

An additional information 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'.[83] Opaque wording and technical terms are the norm for software and hardware contracts, and initial research indicates that this has not changed for eObjects.[84] The content of the information provided may be accurate, but if it is not intelligible to the average consumer, then it is insufficient 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.[85] Careless drafting practices 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 older technologies, and has not been

[82] Coll and Simpson, *Connection and Protection in the Digital Age* (n 2) 37.
[83] Organization for Economic Co-Operation and Development, *Consumer Policy Toolkit* (June 2010) 10.
[84] See the analysis of the Nest thermostat contractual arrangements in Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[85] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).

properly redrafted for eObjects.[86] There is also a common practice in information technology contracts where wording drafted for one jurisdiction is used for contracts made subject to the laws of another jurisdiction. For example, US standard drafting is commonly used in European[87] and Australian[88] contracts, even when it is not particularly suited to the task. This latter issue is not a new phenomenon for eObjects, but it adds to the problems of maintaining compliance with the CPPs of **Information** and **Fairness**.

iii. Delivery mechanism

> Behavioural economics has demonstrated that, among other things, 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.[89]

One of the clearest themes emerging from early visions[90] of ubiquitous computing was the idea that technology should merge into the background, so we do not consciously comprehend our interaction with it. An eObject or a system in which eObjects participate may be designed so that interactions are *invisible* or at least unobtrusive (as discussed above). This unobtrusiveness is often achieved by the absence or miniaturisation of text-supporting interfaces such as screens, which cannot sensibly be used for the delivery of most contractual terms and conditions.

In some cases, this does not matter. Suppliers can easily provide a hyperlink to contractual terms and conditions when an eObject is ordered online, or printed terms and conditions 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 make it likely that there will be a significant 'lack of proximity between consumers, contract terms and the contract formation process', a phenomenon labelled 'Contract Distancing'.[91] Contract Distancing practices mean that consumers

---

[86] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[87] Noto La Diega and Walden, 'Contracting for the "Internet of Things"' (n 41).
[88] This observation is from the author's own experience as a solicitor in Australia specialising in commercial negotiation of information technology contracts.
[89] Organization for Economic Co-Operation and Development, *Consumer Policy Toolkit* (June 2010) 10.
[90] Mark Weiser, 'The Computer in the 21st Century' (1991) Scientific American 94, 94.
[91] 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, 843.

may enter into contracts with a significant limitation on their access to terms and conditions, and consequently consumers have a reduced ability to understand the bargain they are making. Contract Distancing practices are not only seen in the initial contract formation process; they are also seen where initial contracts allow for unilateral amendments by the provider network.

Clear delivery of the full terms before purchase is not ubiquitous in eObjects. Consumers may be given the price upfront when they first purchase the product, but they may not be presented with other terms and conditions (such as EULAs, service agreements and maintenance agreements) until well into the set-up process; that is, after the product has been ordered, delivered, unpacked and partially or even fully set up.

Therefore, consumers may face challenges in finding out the terms and conditions applicable to their eObject, particularly in relation to the use of data. For example, Peppet's 2014 survey of 20 commercially available consumer eObjects found that suppliers had not included anything in the box or packaging relating to data, privacy or security for any of these products.[92] Even in cases where the relevant terms and conditions were displayed on the website, many of these eObjects 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.

If consumers are not receiving proper notification of contractual terms due to Contract Distancing, the **Information** CPP will be breached. 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; therefore, a question about the CPP of **Fairness** may also be raised. **Fairness** is further compromised if Contract Distancing is combined with a right to unilateral amendment by a supplier without a corresponding consumer right to terminate without penalty, such as in some fixed-term contracts.

[92] Peppet, 'Regulating the Internet of Things' (n 6) 141 and Appendix 1.

b. Complexity's effect on Redress

The complexity of eObject ecosystems will often mean it is difficult to allocate liability for particular faults. Even where liability is clear, the mobile nature of eObjects and the differing locations of actors in the provider network mean that practical enforcement may be difficult. This is particularly the case for Commonwealth consumers, as most eObjects purchased by them will be imported, and therefore the contracts will mostly likely contain a choice of foreign jurisdiction and choice of foreign law clauses. These impediments, combined with the usually relatively low value of a consumer claim as compared with likely legal costs, will form a significant barrier to consumers achieving **Redress**.

The complexity of the technology and the complexity of the contractual arrangements both produce a significant challenge for consumers. Defects in an eObject ecosystem causing detriment to consumers can arise in a number of different places: for example, physical faults in the dominant object, faults in the embedded computer hardware, bugs in the software, corruption or deletion of data, or failure of network connections, just to name a few. And the overall detriment may well arise from a combination of defects. For example, a network failure at a critical time may well have corrupted data, which causes the eObject to fail to recognise critical inputs.

If there is one supplier who has provided all of the hardware, software and associated services, then liability allocation is a relatively simple exercise, limited only by whether or not the particular type of harm is legitimately excluded under the contract. But where there is more than one party in the provider network, then the question becomes more uncertain. Where there are entities from multiple jurisdictions involved, with different rules as to allocation of liability (under tort, contract or statutory provisions), these uncertainties become even greater. Contract drafters for provider networks will also inevitably attempt to avoid liability, such as through the use of favourable jurisdiction and choice of law clauses, or arbitration and class action waivers, as is already common in conventional ecommerce.

All of these uncertainties will most likely provide barriers to proper **Redress** for consumers, particularly in relation to low-value contracts. However, consumers are not the only ones who may be detrimentally affected. Uncertainty as to the extent of

legal liability by members of the provider network may well hinder investment and innovation in eObjects.[93]

D. Conclusion

This paper has identified a number of challenges for consumers in consumer transactions arising out of new things, activities and relationships made possible by eObjects that bear further investigation and analysis in Commonwealth and other jurisdictions as to whether they are likely to give rise to legal problems. 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 if vested interests are left unchecked for too long.[94]

It is important to note that the fact that consumers may have challenges to face does not automatically imply that legal problems exist in particular jurisdictions. Depending on the jurisdiction, legislation or other rules may exist that have direct application to the new activities, things or relationships causing consumers concern. Even in circumstances where there are no decided cases that discuss that law's application to eObjects, such a law could still exist.[95] For example, both contract law principles and the consumer protection provisions applicable in Commonwealth countries such as Australia and the United Kingdom are generally quite broad and generic, and are, at least to some extent, not technologically specific.

However, the challenges identified are not just mere inconveniences to consumers. This paper is intended to lay the basis for further examination of particular laws in the Commonwealth and elsewhere, as to whether or not these challenges are currently addressed, in whole or in part, by the law in specific jurisdictions. Early literature on eObjects made it clear that laws concerning consumer privacy need to be a priority for further examination. [96] However, this paper goes past a focus on privacy to examine

[93] Hon, Millard and Singh, *Twenty Legal Considerations for Clouds of Things* (n 35) 18 citing European Commission, *A Digital Single Market Strategy for Europe – COM(2015) 192 final* (2015), para 4.1.
[94] Manwaring, 'Kickstarting Reconnection' (n 1).
[95] Bennett Moses, 'Recurring Dilemmas' (n 1) 252–53.
[96] See n 6.

other areas that could pose problems. Laws concerning safety and quality also need urgent examination in order to deal with widespread security problems already evident in eObjects, and particularly the potential for physical harm. 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. Less evident in current technologies, but likely to be a concern as technologies develop and become more prevalent, is the potential for unfair marketing practices that target already vulnerable consumers or even create them. It is also important that consumer access to appropriate redress for breaching other consumer protection principles be protected, as this forms the foundation of the efficacy of those other principles.

Acknowledgements: The author thanks Associate Professor Lyria Bennett Moses, Professor Roger Clarke and Professor Leon Trakman of UNSW Law School, for their helpful comments on earlier versions of this paper. However, all errors and omissions are the author's own.

References

Barcena MB, Wueest C and Lau H, *How Safe is Your Quantified Self?* (Symantec Security Response Report, 11 August 2014)

Bennett Moses L, 'Recurring Dilemmas: The Law's Race to Keep Up With Technological change' (2007) 2 University of Illinois Journal of Law, Technology & Policy 239

Bilton N, 'Bits Blog: Disruptions: As New Targets for Hackers, Your Car and Your House' *The New York Times* (11 August 2013) < http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0 > accessed 2 Feb 2017

Burrell J, 'How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms' (2016) Big Data & Society 1

Calo R, 'Digital Market Manipulation' (2014) 82 The George Washington Law Review 995

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

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

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

Cloud Security *Security Guidance for Early Adopters of the Internet of Things (IoT)* (April 2015)

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)

Complaint, *NP v Standard Innovation (US) Corp*, Case No 1:16-cv-08655, in the US District Court for the Northern District of Illinois

Consumers International, *The State of Consumer Protection Around the World 2013*

Corkery M and Silver-Greenberg J, 'Miss a Payment? Good Luck Moving That Car' *The New York Times* (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 Feb 2017

Coulouris GF and others, *Distributed Systems: Concepts and Design* (Addison-Wesley 2012)

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

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

European Commission, *A Digital Single Market Strategy for Europe – COM(2015) 192 final* (2015)

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

Federal Trade Commission, *The Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, 2015)

Franceschi-Bicchierai L, 'A GPS Tracker for Kids Had a Bug That Would Let Hackers Stalk Them' (2 February 2016) < http://motherboard.vice.com/read/a-gps-tracker-for-kids-had-a-bug-that-wouldlet-hackers-stalk-them > accessed 20 June 2016

Gibbs S, 'iOS9 Making Your iPhone Slow? You're Not Alone' *The Guardian* (24 September 2015) < https://www.theguardian.com/technology/2015/sep/24/iphone-slow-ios-9-update-iphone-4s-iphone-5-iphone-5s > accessed 12 January 2017

Greenberg A, 'Hackers Remotely Kill a Jeep on the Highway – With Me in It' Wired (21 July 2015) < http://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) < https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/ > accessed 20 June 2016

Halliday J and Lam R, 'Internet of Things: Just Hype or the Next Big Thing? Part II' (2016) 34 Communications Law Bulletin 4

Hartzog W and Selinger E, 'The Internet of Heirlooms and Disposable Things' (2016) 17 North Carolina Journal of Law & Technology 581

Helberger N, ''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)

Heydon G and Zeichner F, *Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act* (Industry Report, Communications Alliance Ltd, October 2015)

Hill K, 'Crib Cams: Watch Out New Parents – Internet-connected Baby Monitors are Easy to Hack' Fusionnet (3 September 2015) < http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/ > accessed 1 March 2015

Hon WK, Millard C and Singh J, *Twenty Legal Considerations for Clouds of Things* (4 January 2016) Queen Mary School of Law Legal Studies Research Paper 216/2016 < http://dx.doi.org/10.2139/ssrn.2716966 >

Kang J and Cuff D, 'Pervasive Computing: Embedding the Public Sphere' (2005) 62 Washington and Lee Law Review 93

Kim NS, 'Two Alternate Visions of Contract Law in 2025' (2014) 52 Duquesne Law Review

Krebs B, Brian Krebs, 'KrebsOnSecurity Hit With Record DDoS' (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) < http://www.healthcare-informatics.com/news-item/cybersecurity/report-internet-enabled-medical-devices-becoming-bigger-target-ransomware > accessed 13 January 2017

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

Leveson NG and Turner CS, 'An Investigation of the Therac-25 Accidents' (1993) 26 Computer 18

Manwaring K, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2016) 21 Deakin Law Review (forthcoming)

Manwaring K and Clarke R, 'Surfing the Third Wave of Computing: A Framework for Research into Networked eObjects' (2015) 31 Computer Law & Security Review 586

Montgomery-Downs H, Insana S and Bond J, 'Movement Toward a Novel Activity Monitoring Device' (2012) 16 Sleep Breath 913

Noto La Diega G, '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

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

Open Web Application Security Project, 'OWASP Internet of Things Project' (2014) < https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29 > accessed 12 January 2017

Organization for Economic Co-Operation and Development, *Consumer Policy Toolkit* (June 2010)

Peppet SR, 'Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts' (2012) 59 UCLA Law Review 676

Peppet SR, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent' (2014) 93 Texas Law Review 85

Productivity Commission, *Review of Australia's Consumer Policy Framework* (Final Report, Canberra 2008) vol 2

Rahman M, Carbunar B and Banik M, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) arXiv:13045672 [csCR]

Reddy T, '15 Companies From Airports to Retail Already Using Beacon Technology' < https://www.umbel.com/blog/mobile/15-companies-using-beacon-technology/ > accessed 10 November 2014

Ridge J, 'What Happens When Everything Becomes Connected: The Impact on Privacy When Technology Becomes Pervasive' (2007–2008) 49 South Texas Law Review

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

Satyanarayanan M, 'Fundamental Challenges in Mobile Computing' (1996) *Principles of Distributed Computing: Proceedings of the Fifteenth Annual ACM Symposium* 1

Schneier B, 'The Internet of Things is Wildly Insecure – and Often Unpatchable' Wired (1 June 2014) < http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/ > accessed 17 December 2015

Stone B, 'Amazon Erases Orwell Books From Kindle' *The New York Times* (18 July 2009) < http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html > accessed 18 May 2016

Thierer AD, 'The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation' (2015) 21 Richmond Journal of Law & Technology

Townsend AM, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia* (W. W. Norton & Company 2013

United Nations Conference on Trade and Development, *Implementation Report on the United Nations Guidelines on Consumer Protection (1985–2013)*

United Nations General Assembly, *United Nations Guidelines for Consumer Protection* (2015)

Uteck A, 'Reconceptualizing Spatial Privacy for the Internet of Everything' (PhD thesis, University of Ottawa 2013)

Vulkanovski A, *"Home, Tweet Home": Implications of the Connected Home, Human and Habitat on Australian Consumers* (Australian Communications Consumer Action Network, Sydney, February 2016)

Walker Smith B, 'Proximity-Driven Liability' (2013–2014) 102 Georgetown Law Journal 1777

Weiser M, 'The Computer in the 21st Century' (1991) Scientific American 94

Wendehorst C, '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)

Wood J, 'iBeacon: the Future of Content Marketing?' B2B Marketing < http://www.b2bmarketing.net/blog/posts/2014/02/17/ibeacon-future-content-marketing > accessed 17 February 2014

Wright D and others (eds), *Safeguards in a World of Ambient Intelligence*, vol 1 (The International Library of Ethics, Law and Technology, Springer 2008)

Zetter K, 'Medical Devices That are Vulnerable to Life-threatening Hacks' Wiredcom < http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x > accessed 3 May 2016

Appendix – core and common attributes of eObjects[97]

CORE ATTRIBUTES

Object – physical object, natural or artificial, inert or living

Computer – contains one or more general-purpose programmable computers

Embedded – one or more computers physically embedded

Data-Collection – contains one or more sensors that can collect or generate data

Data-Handling – capability to process data

Data Communication – can communicate with other nodes inside the same object, or with other objects

COMMON ATTRIBUTES

Active capacity – can act on physical world

Adaptability - context-aware

Addressability – has an unique address

Associability with living beings – humans, plants, animals

Autonomy – decision-making capabilities

Dependency – remote services or infrastructure

Geo-Locatability – can be found in physical space

Identifiability – has an identifier for the physical object

Network Locatability – locatable in virtual space

Mobility – can operate while moving

Operational, economic and social impact – eObjects have both benefits and detriments

Portability – object can be moved but no connectivity while mobile

Prevalence – pervasive or ubiquitous

[97] Appendix reproduced with permission from Manwaring, 'Kickstarting Reconnection' (n 1).

Use pattern – used by an individual, or small numbers, or large numbers

Visibility – can be unobtrusive or invisible, or contain different levels of implicit human-computer interaction **(HCI)**

Volatility – connectivity, energy, storage and processing capabilities may be limited or intermittent

Vulnerability – risk of security breaches, theft, and physical damage or destruction