Emerging information technologies: challenges for consumers

Kayleen Manwaring

To cite this article: Kayleen Manwaring (2017) Emerging information technologies: challenges for consumers, Oxford University Commonwealth Law Journal, 17:2, 265-289, DOI: 10.1080/14729342.2017.1357357

To link to this article: https://doi.org/10.1080/14729342.2017.1357357

Published online: 17 Aug 2017.

Submit your article to this journal

Article views: 71

View related articles

View Crossmark data
Emerging information technologies: challenges for consumers

Kayleen Manwaring

School of Taxation & Business Law, UNSW Business, University of New South Wales, Sydney, Australia

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.

ARTICLE HISTORY Received 1 February 2017; Accepted 15 May 2017

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

1. 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. As these technologies become more prevalent, legislatures, policy-makers 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 make the use of all or any one of these terms problematic. To avoid these problems, in this paper I adopt Manwaring and Clarke’s approach developed in 2015, and use the term ‘eObjects’ (enhanced objects), which is more fully defined in Section 2.

Most of the discussion of eObjects to date has concentrated on the inadequacy of existing privacy and data protection laws. 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. 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. These challenges can arise not only in relation to the attributes of eObjects themselves, but also out of contractual arrangements used to supply them to consumers.

Section 2 of this paper outlines the scope of the emerging technologies discussed in this paper and provides a definition of ‘eObject’. Section 3 describes a set of consumer protection principles (CPPs) derived from the recently revised United Nations Guidelines for Consumer Protection (2015 Guidelines). Section 4 uses the eObjects framework summarised in Section 2 to identify the challenges consumers may face when entering into a contract relating to eObjects. Section 4 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. Section 5 concludes the article by highlighting some of the most important legal areas that bear further investigation in individual jurisdictions.

2. eObjects and the socio-technical landscape

In short, an eObject (as defined by Manwaring and Clarke) 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.

Such a shorthand definition, while helpful, cannot be complete, considering the variety and complexity of the technologies involved. eObjects already appear in many industries, including transport, utilities, healthcare, building, industrial and home automation, agriculture, fitness and lifestyle, toys, entertainment, consumer appliances, logistics, sport, security and art. Many examples of eObjects are discussed in this paper, including Internet-connected kettles, cars, fitness trackers, heart defibrillators, children’s and adults’ toys, guns, locks, e-book readers, fridges and thermostats, but there are many more.

To focus attention for further research and give a more complete view of the technologies, Manwaring and Clarke developed a framework with three dimensions: core attributes, interactions and common attributes. The core attributes are italicised in the definition above. Four key types of interactions with eObjects were also identified: living things, the physical world, other eObjects, etc.
and other computing devices or systems. Common attributes of eObjects do not appear in all eObjects, and even where they do appear, the nature and significance of their effect can vary. However, the italicised attributes below have been identified because they appear sufficiently frequently, and have such effects, that they are capable of driving significant socio-technical change either by themselves or (more likely) in combination with other attributes or interactions. These common attributes are: active capacity (capability to act on the physical world), adaptability (context-awareness), addressability (unique address), associability with living beings, autonomy, dependency (on remote services or infrastructure), geo-locatability, identifiability (unique device identifier/s), mobility or portability, operational, economic and social impact, network locatability, prevalence, use pattern, visibility, volatility and vulnerability.

This framework with its italicised attributes is used in Section 4 to identify the challenges consumers may face when acquiring eObjects.

### 3. 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). The 2015 Guidelines contain a set of principles intended to describe ‘the main characteristics of effective consumer protection legislation, enforcement institutions and redress systems’. These CPPs can be summarised as follows.

<table>
<thead>
<tr>
<th>Section of 2015 Guidelines</th>
<th>Description</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>III.5(a), V.E</td>
<td>Consumers should have access to essential goods and services</td>
<td>Essentials</td>
</tr>
<tr>
<td>III.5(b), IV.11(a)</td>
<td>Consumers who are vulnerable or disadvantaged should be protected</td>
<td>Disadvantage</td>
</tr>
<tr>
<td>III.5(c), V.B, V.D</td>
<td>Consumers should be protected against threats to health and safety</td>
<td>Safety</td>
</tr>
<tr>
<td>III.5(d), IV.11(b), V.C</td>
<td>Consumers should be protected against unfair practices, such as misleading marketing practices and unfair contract terms</td>
<td>Fairness</td>
</tr>
<tr>
<td>III.5(d), V.C</td>
<td>Businesses should supply goods and services which are durable, reliable and fit for purpose</td>
<td>Quality</td>
</tr>
<tr>
<td>III.5(e), IV.11(c)</td>
<td>Consumers should be given access to sufficient information to make informed individual choices</td>
<td>Information</td>
</tr>
<tr>
<td>III.5(f), V.G</td>
<td>Consumers should be given access to education programmes</td>
<td>Education</td>
</tr>
<tr>
<td>III.5(g), V.F</td>
<td>Effective dispute resolution and redress should be provided to consumers</td>
<td>Redress</td>
</tr>
<tr>
<td>III.5(h)</td>
<td>Representation</td>
<td>(Continued)</td>
</tr>
</tbody>
</table>

---

11Manwaring and Clarke (n 3) 600–01.
12Ibid.
14UNGA, ‘2015 Guidelines’ (n 8), Preface, 3.
Section of 2015 Guidelines | Description | Abbreviation
--- | --- | ---
III.5(i), V.H | Consumers should be given the freedom to form consumer groups which are allowed to present their views to decision-making bodies | |
III.5(j), V.I | Sustainable consumption by consumers should be promoted | Sustainability
III.5(k) | Consumers using electronic commerce should be given no less protection than is provided in other forms of commerce | Parity
III.5(l) | Consumers’ privacy should be protected | Privacy

The most significant changes introduced by the 2015 Guidelines include:

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

The consumer protection principles contained in the Old Guidelines have generally been adopted, in whole or in part, by UN member states, including Commonwealth countries. 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 consumer protection law in the face of socio-technical change brought about by eObjects.

### 4. 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:

- eObjects are imperfect (see Section 4.1);
- eObjects can be controlled and modified remotely by suppliers and others in the provider network (see Section 4.2);
- eObjects can manipulate or impede consumer choice (see Section 4.3);

---


16I 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.
• eObjects have a significant post-supply value to suppliers and other related goods and services providers (see Section 4.4) and
• eObjects are complex (see section 4.5).

4.1. Imperfection

Suppliers with low profit margins and limited experience in manufacturing computing products may have little incentive or capability\(^\text{17}\) to ensure that eObjects operate reliably. Possible harms to consumers faced with the challenges described in this section raise potential conflicts with the CPPs of Quality and Safety and with other CPPs, as set out below.

4.1.1. Risks of failure

**Vulnerability** is an important attribute of consumer eObjects. In the early days of eObjects, Satyanarayanan argued that eObjects are more prone to physical interference and remote attacks than conventional connected computers.\(^\text{18}\) A deluge of subsequent reports supports this view. Security vulnerabilities have been identified in: fitness trackers;\(^\text{19}\) medical eObjects such as insulin pumps, heart defibrillators and CT scanners;\(^\text{20}\) domestic appliances such as Internet-connected kettles,\(^\text{21}\) baby monitors,\(^\text{22}\) children’s toys\(^\text{23}\) and location trackers;\(^\text{24}\) as well as guns\(^\text{25}\) and cars,\(^\text{26}\) just to name a few.

---

\(^{17}\)Peppet (n 5) 135–36.


The increased risk of security exploits arises from security vulnerabilities in both the eObjects themselves and the systems to which they are connected; they include inadequate encryption, weak passwords, lack of account lock out, poor authentication, authorisation and updating practices, and lack of physical safeguards.\(^{27}\) The nature of many manufacturers as consumer goods specialists rather than ICT specialists, the small size of many devices, and design flaws prohibiting software patches have all been cited as reasons why security problems arise so commonly in eObjects.\(^{28}\)

Security attacks enabled by 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. In September 2016, the website of security journalist Brian Krebs experienced a distributed denial of service attack delivered primarily through eObjects.\(^{29}\) Of course, such attacks are also delivered using conventional computers; what is more particular to eObjects is the physical harm that might occur to the eObject, surrounding objects and/or living things.\(^{30}\)

The potential for physical harm is likely to emerge when the attribute of vulnerability interacts with that of mobility and/or active capacity. Security researchers have found ways to control connected cars’ locks, brakes, steering and transmission remotely.\(^{31}\) Internet-connected kettles have been exposed as significant security threats.\(^{32}\) Hackers can potentially wrest control from drivers of heavy objects travelling at speed or find an entry point into a smart home where connected sprinklers could be turned off and hotplates turned on. Ransomware, already used to breach the security of medical eObjects,\(^{33}\) offers a financial incentive to threaten such harm.

---


\(^{31}\) See n 26.

\(^{32}\) Cimpanu (n 21).

Many, if not most, eObjects or their associated systems have the attribute of volatility: limited or intermittent access to resources needed to operate, particularly network connections, energy sources and processing power.\(^{34}\) This constraint is a particular challenge for users of mobile eObjects, where the size, weight and form of the eObject dominate design decisions,\(^{35}\) often at the expense of resource allocation. Mobile eObjects currently need to be designed to minimise power usage, which can negatively affect processing power and speed. For simple applications, this constraint may matter little; but for healthcare eObjects, the draining of a power source or the loss of connectivity leading to loss of control can cause serious harm, even death.

### 4.1.2. Risky decision-making: inaccuracy and autonomy

All eObjects can collect, handle and communicate data.\(^{36}\) Data may be or become inaccurate during the eObject’s performance of any of these processes. Sensors can be misled by physical phenomena; algorithms can be wrong; data records can be corrupted. Questions have been raised about the accuracy of accelerometers\(^ {37}\) and sleep trackers.\(^ {38}\)

Consumers, the provider network and others who rely on accurate data (e.g., users and receivers of insulin injections) are, of course, at risk of physical or other harm if such data is inaccurate.\(^ {39}\) 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 were identified in autonomous objects with active capacity. In the mid-80s, two people died and others were injured when computerised radiotherapy machines in hospitals administered massive overdoses of radiation to patients, partially due to an incorrect zero value in a failsafe counter.\(^ {40}\) Although the risks are not new, the increased prevalence of autonomous eObjects can potentially increase the likelihood of such incidents occurring, particularly when such objects are also vulnerable to security breaches.

Even when data are accurate, eObjects with some autonomous decision-making capability are risky. Decision-making algorithms could be

\(^{34}\)George F Coulouris and others, *Distributed Systems: Concepts and Design* (5th edn, Addison-Wesley 2012) 817 ff.

\(^{35}\)Satyanarayanan (n 18) 1.

\(^{36}\)Manwaring and Clarke (n 3).


programmed to result in outcomes not desired by the user. Consumers rarely see 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.\textsuperscript{41}

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. Consider the automatic reordering function in products such as Amazon Dash Buttons:\textsuperscript{42} who is liable to pay if 1,000 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: who is liable for an unfavourable and unwanted contract entered into by a machine, which was not predictable by the machine’s user (or indeed its programmer)?

\textbf{4.1.3. 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 package’,\textsuperscript{43} where services are provided along with the object. 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, and other actors, depending on the complexity of the eObject and the system in which it participates.\textsuperscript{44}

Risk management is complicated by the nature of eObjects as product-service packages, and further so when there are multiple players in the provider network. There are three main challenges:

\begin{itemize}
  \item Proactive management of risk: what are the provider network’s obligations in relation to monitoring and updating of software?\textsuperscript{45}
\end{itemize}


\textsuperscript{42}http://www.amazon.com/Dash-Buttons/b?ie=UTF8&node=10667898011.

\textsuperscript{43}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) 135, 141.

\textsuperscript{44}See eg Guido Noto La Diega and Ian Walden, ‘Contracting for the “Internet of Things”: Looking into the Nest’ (2016) 7 (2) European Journal of Law and Technology 1, for a detailed description of the large number of product and service providers that can be involved in provision and support of an eObject.

\textsuperscript{45}Christiane Wendehorst, ‘Consumer Contracts and the Internet of Things’ in Schulze and Staudenmayer (n 43) 189, 194–95.
When things go wrong: who is responsible for fixing problems with the eObject?\textsuperscript{46}

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 entering 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 how to exploit it on the World Wide Web.

The consumer would be concerned with the following questions:

- Does the provider network undertake any security monitoring?
- Will she be notified if there is a vulnerability? And if so, when?
- Who is responsible for supplying security patches and when will they be available?
- If urgent repair is needed, and either the provisions for repair or the agreed timeframe is inadequate, what rights does she have to bring in a third party to secure the lock? (Any locksmith can fix or replace 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 and 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 judgement on the adequacy of answers to these questions may be essential when choosing between competing products. Information that is not readily available, or is unintelligible or imprecise, 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, this will come into conflict with the CPPs of Safety, Quality and Redress.

4.2. Remote control

The capacity of eObjects for data-handling and data communication, and in some cases their dependency on remote services and infrastructure, exposes

\textsuperscript{46}Wendehorst (n 45) 195–96.
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;
- programme 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.47

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.48 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 in a car 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.49

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.50 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

49Corkery and Silver-Greenberg (n 48).
Capabilities to a level that makes the hardware unusable. 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, 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.

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.

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.

### 4.3. 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

---

52 Wendehorst (n 45) 201–02.
54 Coll and Simpson (n 2) 35–36.
Fairness. Some behaviours may also be incompatible with the CPPs of Disadvantage and Information.

4.3.1. 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.\(^{55}\)

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, 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.\(^{56}\) For example, advertisers may filter the available information; they may target consumers at the time when their willpower is

---


\(^{56}\)Calo (n 6) 1 ff; Kim (n 6) 312; Helberger (n 43) Part II; Eliza Mik, ‘The erosion of autonomy in online consumer transactions’ (2016) 8 Law Innovation and Technology 1, 1 ff; James Halliday and Rebekah Lam, ‘Internet of Things: Just Hype or the Next Big Thing? Part II’ (2016) 34 Communications Law Bulletin 4, 7.
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’.\(^{57}\)

Currently, most examples of digital market manipulation have been identified in conventional ecommerce.\(^{58}\) 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\(^{59}\) 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 it was being used or piloted by retail, fast food, sporting, airline, real estate services, pharmacies and other business enterprises.\(^{60}\)

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.\(^{61}\) 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.\(^{62}\) 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’.\(^{63}\)

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

\(^{57}\)Calo (n 6) 1.

\(^{58}\)Ibid.

\(^{59}\)iBeacon uses the Bluetooth Low Energy communications standard, but other beacon technologies use both Bluetooth and Wi-Fi (eg Motorola Solutions and Datzing).


\(^{61}\)Kim (n 6) 312.

\(^{62}\)Hartzog and Selinger (n 50) 591–92.

\(^{63}\)Helberger (n 43) 160.
practice into something that is considered to be ‘unfair’ persuasion. 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.

4.3.2. 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 about the attributes and interactions of eObjects and their disadvantages, such as in the areas of privacy and security, may find it impossible to opt out.

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.

4.4. Post-supply value
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. 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;

64 Calo (n 6) 1032.
65 Coll and Simpson (n 2) 38.
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’).67

### 4.4.1. 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.68 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 customers … allowing [Standard Innovation] to link the usage information to specific customer accounts.69

67Coll and Simpson (n 2) 47.
68Wendehorst (n 45) 193–94.
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.\textsuperscript{70} This is a clear breach of the new CPP of Privacy, and the litigation was settled on 9 March 2017, for CAD$5 million.\textsuperscript{71}

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:

- are aware of what data are being collected, to whom it will be provided, and for what purpose (‘data awareness’) and
- 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.\textsuperscript{72}

4.4.2. Post-supply restrictions

The fact that eObjects contain a programmable computer with data collection and handling capabilities means that some form of software will be provided in every eObject. Some types of eObjects, such as e-book readers and networked media players, will also contain 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;
- the eObject may not be ‘sold’ to the consumer, in the sense 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;\textsuperscript{73}
- 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

\textsuperscript{69}Complaint, \textit{NP v Standard Innovation (US) Corp} (Case No 1:16-cv-08655, US District Court for the Northern District of Illinois) [19].

\textsuperscript{70}Complaint, \textit{NP v Standard Innovation (US) Corp} (n 69) [23].

\textsuperscript{71}Class Action Settlement Agreement, \textit{NP v Standard Innovation (US) Corp} (n 69).

\textsuperscript{72}Helberger (n 43) 147–51.

\textsuperscript{73}Walker Smith (n 47) 1815–16; Fairfield (n 6) 83; Hon, Millard and Singh (n 39) 16.
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.\(^\text{74}\)

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\(^\text{75}\) and
- more significant penalties for breach of use restrictions, such as those contained in anti-hacking\(^\text{76}\) and/or copyright legislation, as opposed to civil remedies for contractual breach.

For example, if consumers wish to make their own repairs to an eObject, such as a connected vehicle, they may need to access integrated software, and face both legal and technical barriers to do so. Software modification without provider consent will in many cases be 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 itself in jurisdictions signatory to and compliant with the WIPO Copyright Treaty.\(^\text{77}\) Providers might also use their remote disablement capacity (see Section 4.2) to lock down software for a perceived breach of copyright law or contractual conditions.\(^\text{78}\)

These challenges are not merely theoretical. For several years, US farmers have been disputing the attempts of Deere & Company (John Deere) and

\(^\text{74}\)Wendehorst (n 45) 201.
\(^\text{75}\)eg the terms applicable to Amazon’s Alexa virtual personal assistant at [http://www.amazon.com/gp/help/customer/display.html?nodeId=201809740] and [https://www.amazon.com/gp/help/customer/display.html/?nodeId=508088] accessed 10 July 2017.
\(^\text{76}\)Walker Smith (n 47) 1815–16 and fn 313.
\(^\text{78}\)This possibility was suggested by one of the OUCLJ anonymous reviewers.
other manufacturers to restrict their rights to repair their agricultural machinery, which contains embedded software and TPMs.\textsuperscript{79} In 2015, against the objections of John Deere and others,\textsuperscript{80} the US Copyright Office granted a three-year exemption for vehicle software modification to the anti-circumvention provisions of the Digital Millennium Copyright Act\textsuperscript{81} (DMCA).\textsuperscript{82} A year later, John Deere issued a licence agreement which prohibits almost all software modification and circumvention of TPMs,\textsuperscript{83} in what appears to be an attempt to replace its DMCA rights with contractual rights\textsuperscript{84} and ensure that all repairs are done by John Deere contractors.

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 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.

4.5. Complexity

The core attributes of an eObject mean there is no such thing as a ‘simple’ eObject. Each eObject is a hybrid of software, hardware and physical object, usually inseparable,\textsuperscript{85} 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.

Two types of complexity produce challenges for consumers:

\begin{footnotesize}
\begin{enumerate}
\item §1201(a)(1), Title 17, USC.
\item Koebler (n 79).
\item Noto La Diega and Walden (n 44) 8; Coll and Simpson (n 2) 33.
\end{enumerate}
\end{footnotesize}
• the complexity of the technology itself and
• the complexity of the contractual arrangements associated with supply.

The nature of eObject ecosystems promotes the likelihood of numerous actors in the provider network. A complex network means complexity in contractual arrangements and therefore liability allocation. 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. These contracts may be with separate entities, some having no connection with (or knowledge of) others in the network.

The complexity of contractual arrangements within a network can make it difficult to identify all applicable contracts, let alone interpret them for end-consumers (including enterprises) and network actors. For example, the Nest thermostat is sold subject to at least 13 documents stipulating the ‘rights, obligations and responsibilities’ of the various parties in the provider network. Therefore, the likelihood of conflicting terms and conditions is high, as is uncertainty regarding their effects.

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

4.5.1. Making an informed choice

A consumer entering into a contract requires sufficient, accurate and intelligible information on the nature, features and dependencies of the product or service, in order to meet the CPP of Information. A supplier of a simple product needs only provide minimal information to fulfil this requirement. The complexity of eObjects, particularly product-service packages, dictates that more than minimal information is required to sufficiently inform a consumer. And mere provision of information by one supplier is insufficient—the consumer’s knowledge of alternatives on offer and their judgement of the price and quality differences are also required.

Consumers face three main challenges to receiving adequate Information:

• the type of information required (content),

---

86Noto La Diega and Walden (n 44) 4–6.
87Hon, Millard and Singh (n 39) 7.
88Noto La Diega and Walden (n 44) 3.
89Noto La Diega and Walden (n 44) 6.
90Hon, Millard and Singh (n 39) 16–17, citing generally an earlier version of Noto La Diega and Walden (n 44).
92See section 4.5.1.1.
• whether the consumer can adequately understand the information provided (intelligibility)\(^{93}\) and
• when and how the information is provided (delivery mechanism).\(^{94}\)

4.5.1.1. Content. Consumer knowledge of the eObject’s functionality is important, as is its suitability for the consumer’s particular purposes. Knowledge of ‘normal’ functionality is usually insufficient, particularly for eObjects with significant volatility and/or dependencies: such eObjects face significant limitations on functionality in particular situations.\(^{95}\)

Knowing exactly what the eObject does enables consumers to assess whether it meets their needs. This knowledge is also important because the post-supply value of eObjects (particularly data collection) can incentivise suppliers to include features that benefit the supplier or others in the provider network but are a disbenefit to consumers and therefore affect their purchasing decision. Such functionality may be invisible or unobtrusive; overt disclosure of this ‘dark’\(^{96}\) functionality may need to be formally required, otherwise consumers may remain unaware of it, as in the We-Vibe example above.

Aside from functionality, the attribute of dependency and the nature of eObject interactions mean specific information on interoperability is often critical. A smart kettle that cannot connect to a particular type of home network has limited utility. If a homeowner is not told the kettle is only usable if connected through the homeowner’s mobile network (with associated higher data costs), the bargain may be substantially different to what they expect. Alternatively, particular systems may only allow add-in of particular brands of eObjects,\(^{97}\) thereby restricting consumers’ freedom of choice.

Clear information on price is fundamental to any consumer contract. This includes not just the price of initial supply, but also follow-on costs, such as purchase of additional applications, subscription fees for service agreements and costs of consumables. Consumers should also be aware of non-money considerations, such as post-supply obligations, for example in relation to data and use restrictions.

Ascertaining payment terms and the consequences of failure to pay may also be problematic, particularly when billing is done by more than one

\(^{93}\)See section 4.5.1.2.
\(^{94}\)See section 4.5.1.3.
\(^{95}\)Wendehorst (n 45) 191–92.
\(^{96}\)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 (The International Library of Ethics, Law and Technology, Springer 2008).
\(^{97}\)Coll and Simpson (n 2) 37.
provider network entity. Payment terms, such as due dates and price increases, may vary greatly between entities.

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

4.5.1.2. 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’.98 Opaque wording and technical terms are the norm for software and hardware contracts, and initial research indicates this has not changed for eObjects.99 The content provided may be accurate, but if it is not intelligible to the average consumer, it is insufficient to enable an informed choice.

Consumers also find contractual terms and conditions difficult to understand.100 Careless drafting adds to the problem. Researchers have identified terms and conditions in contracts involving eObjects that contain wording obviously written for older technologies and not properly redrafted.101 A common practice in information technology contracts is to use wording drafted for one jurisdiction in contracts made for another. US standard drafting is commonly used in European102 and Australian103 contracts, even when not particularly suitable. This latter issue is not new for eObjects, but it adds to problems of complying with the CPPs of Information and Fairness.

4.5.1.3. 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.104

A clear theme of early visions105 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.106 This is often achieved by removing or miniaturising text-supporting

99See the analysis of the Nest thermostat contractual arrangements in Noto La Diega and Walden (n 44)6ff.
100ibid 3, 9.
101ibid 3.
102ibid.
103This observation is from the author’s own experience as a solicitor in Australia specialising in commercial negotiation of information technology contracts.
104OECD (n 98) 10.
106See section 4.5.1.1 above.
interfaces such as screens. Such interfaces cannot practically be used to deliver most contractual terms and conditions.

In some cases, this does not matter. Suppliers can provide a hyperlink to the terms and conditions when an eObject is ordered online, or provide printed terms and conditions over the counter or in the box for a bricks-and-mortar purchase. However, in other cases, the contractual processes encourage ‘lack of proximity between consumers, contract terms and the contract formation process’, a phenomenon labelled ‘Contract Distancing’.107 Contract Distancing leads to consumers entering into contracts with significantly limited access to terms and conditions and, consequently, a reduced ability to understand the bargain. Contract Distancing practices are seen both at contract formation and where initial contracts allow for unilateral amendments by the provider network.

Clear delivery of full terms before purchase of eObjects is not ubiquitous. Consumers may be given the price upfront on purchasing the product, but 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 data usage. 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.108 While the relevant terms and conditions were displayed on the website, many eObjects were bought in bricks-and-mortar stores. Therefore, consumers were at risk of buying these eObjects without any knowledge of those terms, as there was no clear indication the purchase was subject to further terms and conditions.

If consumers do not receive proper notification of contractual terms due to Contract Distancing, the Information CPP is breached. Contract Distancing also removes the notification some steps away from the actual transaction, raising a question about the CPP of Fairness. Fairness is further compromised if Contract Distancing is combined with a supplier’s right to unilateral amendment without a corresponding consumer right to terminate without penalty, as in some fixed-term contracts.

4.5.2. Complexity’s effect on redress
The complexity of eObject ecosystems can hamper the allocation of liability for faults. Even where liability is clear, the mobile nature of eObjects and

108Peppet (n 5) 141, 167–78.
the differing locations of provider network actors can make practical enforcement difficult. Commonwealth consumers are particularly affected, as most eObjects they purchase are imported, with contracts likely to contain foreign jurisdiction and foreign law clauses. These impediments, combined with the usually low value of a consumer claim relative to legal costs, often hinder consumers achieving Redress.

The complexity of the technology and the contractual arrangements produces a significant challenge for consumers. Defects in an eObject ecosystem causing detriment to consumers can arise in several places, including physical faults in the dominant object or embedded computer hardware, bugs in the software, corruption or deletion of data or failure of network connections. And the overall detriment may arise from a combination of defects, as where a network failure corrupts data, causing the eObject to fail to recognise critical inputs.

Where a single supplier provides the hardware, software and associated services, liability allocation is relatively simple, limited only by whether the type of harm is legitimately excluded under the contract. But where there are multiple providers, the issue becomes uncertain. And where entities from multiple jurisdictions are involved, with different rules for allocating liability (under tort, contract or statutory provisions), this uncertainty multiplies. Contract drafters for provider networks also inevitably attempt to avoid liability, using favourable jurisdiction and choice of law clauses, or arbitration and class action waivers—practices already common in conventional ecommerce.

All of these uncertainties are likely to obstruct proper Redress for consumers, particularly in relation to low-value contracts. However, consumers are not the only ones facing detrimental effects. Uncertainty about the legal liability of provider network actors may hinder investment and innovation in eObjects.109

5. 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 overregulation, the second is the cementing of socially undesirable outcomes if vested interests are left unchecked for too long.110

110 Manwaring (n 1).
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. For example, both contract law principles and the consumer protection provisions applicable in Commonwealth countries such as Australia and the UK 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. However, this paper goes past a focus on privacy to examine other problematic areas. Laws concerning safety and quality also need urgent examination 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 CPPs be protected, as this forms the foundation of the efficacy of those other principles.

Acknowledgements

The author thanks Associate Professor Lyria Bennett Moses and Professor Leon Trakman of the University of New South Wales Law School, for their helpful comments on earlier versions of this paper. She also thanks the anonymous reviewers for their useful feedback and Marie-Louise Taylor and Lilla Wendoloski for their editing assistance. However, all errors and omissions are the author’s own.

Notes on contributor

Kayleen Manwaring is a lecturer at the University of New South Wales, School of Taxation and Business Law.

111 Bennett Moses (n 1) 252–53.
112 See n 5.