From:	Kayleen Manwaring
To:	iotrfc2017
Subject:	FW: Internet of Things Request for Comment 2016 - Submission by Kayleen Manwaring, University of New South Wales Australia
Date:	Sunday, February 05, 2017 6:12:20 PM
Attachments:	image001.jpg image002.jpg image003.jpg image004.jpg image005.jpg Kickstarting reconnection.pdf

---

Internet of Things Request for Comment 2017 - Submission by Kayleen Manwaring, UNSW Sydney

As a response to Question 1 of the 13 Jan 2017 Notice for Request for Comment, I attach my forthcoming article in *Deakin Law Review* which sets out some additional challenges for the IoT that should be considered.

Kind regards

Kayleen Manwaring | Lecturer | School of Taxation & Business Law (incorporating Atax)
UNSW Business School | UNSW Sydney
Room 2068 | Level 2, Quadrangle Building (E12) | UNSW Sydney 2052
Telephone: +61 (2) 9385 7631 | Fax: +61 (2) 9313 6658 | Web: www.business.unsw.edu.au

Undergraduate Business Law courses (School of Taxation & Business Law)
Postgraduate Business Law courses (School of Taxation & Business Law)

View some of my research on my SSRN Author page:
http://ssrn.com/author=1848279

Member of UNSW's Law, Technology and Innovation research network -
http://www.law.unsw.edu.au/centres/networks-groups/law-technology-and-innovation-research-network

UNSW Business

Manwaring, K, (2016) "Kickstarting reconnection: an approach to legal problems arising from emerging technologies", *Deakin Law Review*, Vol 21 Iss 2 (forthcoming)

Kayleen Manwaring[1]

Abstract

A new model, or 'third wave', of computing is emerging, based on the widespread use of processors with data handling and communications capabilities embedded in a variety of objects and environments that were not previously computerised. Various terms have been used to describe this third wave, including 'ubiquitous' and 'pervasive' computing, 'ambient intelligence', the 'Internet of Things' and 'eObjects'. With the socio-technical change brought about by this third wave comes the possibility of a disconnection between the law and the new things, activities, and relationships enabled by this new model of computing. This disconnection may lead to legal problems of uncertainty, under- or over-inclusiveness of conduct in existing law, obsolescence, or the complete absence of laws regulating new behaviour. Early and rigorous identification and categorisation of legal problems is crucial for emerging technologies, to assist in avoiding two problems: the first being the stifling of beneficial innovation by over-regulation, the second the cementing of socially undesirable outcomes when vested interests are left too long unchecked. Although the technologies in the third wave are diverse, common attributes can be identified, and from examination of these attributes significant innovations are revealed. This paper examines these innovations to assist in identifying legal problems arising from the third wave.

1 Introduction

> [A]s technology changes, legal dilemmas arise. As technological change becomes increasingly rapid, the need for a methodological approach to these problems becomes increasingly urgent.[2]

Beginning with Mark Weiser in the early 1990s, commentators have been predicting the widespread consumer and commercial adoption of 'a third wave of computing'. This third wave encompasses the development and commercial and consumer use of previously unconventional forms of distributed information technologies, including smartphones, wearable computers and human ICT implants. This third wave contemplates a socio-technical shift where access to networked computing is no longer confined to desktop machines, but where sensors and microprocessors with internetworking capabilities are embedded in everyday objects and environments not previously computerised, such as cars, fridges, people and animals. The technologies that make up the third wave are referred to as "eObjects" (enhanced objects) in this paper, and this term is more fully described in Part 2.1 and the Appendix.

---

[1] Lecturer, School of Taxation & Business Law, UNSW Business, UNSW Australia. The author thanks the anonymous reviewer, Associate Professor Lyria Bennett Moses, Professor Roger Clarke and Professor Leon Trakman of UNSW Law School, and Stuart Dowling of Honeywell Ltd, for their helpful comments. Thanks also to Lyn Dowling for her proofreading assistance. However, all errors and omissions are the author's own.

[2] 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, 285.

With the socio-technical shift brought about by the emergence of eObjects, comes the possibility of disconnections between existing law and the new things, activities, and relationships that arise out of the development and use of these new technologies. In Australia, there is as yet very little judicial, and no legislative or governmental analysis of the possibility of disconnections.[3] Part 2.2 of this paper outlines significant imperatives for legal researchers and law reform agencies to uncover and respond to possible disconnections quickly and rigorously. It continues on to identify the categories of legal problems that might arise because of the new things, activities and relationships made possible by eObjects. It also proposes that the most fruitful way to begin an analysis of legal problems is through identification and examination of the innovations that arise out of the attributes of eObjects. Part 3 goes onto identify some key innovations arising out of particular attributes of eObjects identified in Part 2.1, and the interactions between them. It then explains and categorises useful examples of existing and potential legal problems arising out of these key innovations.

The main purpose of this paper is to provide legal researchers and law reform agencies a useful analytical approach to take when faced with socio-technical change, and to illustrate its use in a particular context, that of socio-technical change brought about by eObjects. This approach also assists in identifying the diversity of legal problems that may arise in this context, in contrast with the majority of the existing literature, which concentrates mainly on the implications of eObjects for privacy and security.[4] It is not possible within the scope of this paper to be comprehensive, due to the nature and variety of innovations within eObjects and possible effects on the law. However, the approach taken to analysing the legal problems can provide a roadmap for further research that concentrates on more confined issues and/or legal areas in depth.

2 The interaction between socio-technical change and law

> The current state of technology limits, in practice, what actions we *can* perform, what objects we *can* create, and what relationships we *can* form. It is thus common for

[3] However, two Australian industry and consumer bodies have issued reports: Geof Heydon and Frank Zeichner, ''Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act' (Industry Report, Communications Alliance Ltd, October 2015)' ; Alexander Vulkanovski, ''*"Home, Tweet Home"*: Implications of the Connected Home, Human and Habitat on Australian Consumers', report for Australian Communications Consumer Action Network (ACCAN), Feb 2016' (2016)

[4] Eg Scott R Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent' (2014) 93(1) *Texas Law Review* 85; Anne Uteck, *Reconceptualizing Spatial Privacy for the Internet of Everything* (PhD thesis Thesis, University of Ottawa, 2013); Robert M. Davison, 'The privacy rights of cyborgs' (2012) 27 *Journal of Information Technology* 324; Adam D. Thierer, 'The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation' (2015) 21(2) *Richmond Journal of Law & Technology* ; Grace Li, 'Deciphering Pervasive Computing: a Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' in Varuna Godara (ed), *Risk Assessment and Management in Pervasive Computing: Operational, Legal Ethical and Financial Perspectives* (Information Science Reference, 2009) 218-245; Varuna Godara (ed), *Risk assessment and management in pervasive computing operational, legal, ethical, and financial perspectives* (Information Science Reference, 2009) ; Kevin King, 'Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 *Albany Law Journal of Science & Technology* 61; Nancy J King, 'When Mobile Phones Are RFID-Equipped — Finding EU-US Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce' (2008) 15 *Michigan Telecommunications & Technology Law Review* 107; Rolf H. Weber, 'Internet of things – New security and privacy challenges' [23] (2009) 26(1) *Computer Law and Security Review: The International Journal of Technology and Practice* 23; David Wright et al (eds), *Safeguards in a world of ambient intelligence* (Springer, 2008) vol 1,

> technological change to impact the law, which limits what actions we *may* perform, what objects we *may* create and use, and what relationships *will* be recognized.[5]

2.1 The nature of eObjects

The technologies making up the 'third wave' have been called a number of different names, most commonly 'ubiquitous' and 'pervasive' computing, 'ambient intelligence', and the 'Internet of Things'. Unfortunately, both popular and academic writers have been inconsistent in their use of these terms. Definitions have varied depending on geographical locations, individual researchers, and have also changed over time. To deal with these limitations, this paper adopts the approach taken by Manwaring and Clarke,[6] who recently undertook a historical and critical analysis of the different terminologies. They proposed a new term, 'eObject', for the central element of these new technologies. An eObject ('enhanced object') is an:

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

However, the technologies and their effects are complex, so this definition, while useful as a starting point, does not give a complete view of the technologies that the literature discusses. With this limitation in mind, Manwaring and Clarke also derived in addition to the core definition, a list of common attributes of eObjects. These common attributes, although they do not appear in all eObjects, appear sufficiently frequently to drive significant socio-technical change, and are therefore useful to examine when exploring legal, business strategy, and public policy problems that might arise. These common attributes include technical attributes such as volatility of resources and vulnerability to security breaches, as well as functional attributes such as increased mobility of devices and people, the change in the geographical extent of technology, the use of context-aware and autonomous decision-making technologies, and the likelihood of decreased visibility of devices due to advancements in implicit human computer interaction, just to name a few. A full list of these attributes is set out in the Appendix.

2.2 An approach to uncovering legal problems in the face of socio-technical change

The concept of 'socio-technical change' used in this paper acknowledges that relevant change does not arise only in circumstances where a new product or process is developed or an existing product or process is modified. Socio-technical change also occurs where new forms of **conduct** enabled by new or modified technologies emerge to form part of social practice. [7] Where particular socio-technical changes have significant impacts, questions about how law and other regulatory tools should respond will inevitably be asked. In

---

[5] Lyria Bennett Moses, 'Why have a theory of law and technological change?' (2007) 8(2) *Minnesota Journal of Law, Science & Technology* 589

[6] Kayleen Manwaring and Roger Clarke, 'Surfing the third wave of computing: a framework for research into networked eObjects' (2015) 31(5) *Computer Law & Security Review* 586

[7] Lyria Bennett Moses, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1, 10.

particular, should the new actions, products and/or relationships brought into being be permitted, prohibited, encouraged, required[8] or limited in some way? And if so, how?

Changes to law or other forms of regulation should of course be approached cautiously. Failure to prohibit particular activities may lead to socially undesirable results,[9] such as allowing unlimited surveillance of private spaces. However, 'premature, over-reaching or excessive lawmaking may … be an option worse than doing nothing', particularly where investment in beneficial new technologies may be unnecessarily fettered or driven offshore by regulatory interference and compliance costs.[10] It is also important to remember that just because a technology is new, or significantly changed, does not by itself mean that its applications operate outside of the scope of existing law.[11] A new technology, especially in the ICT industry, rarely emerges completed ungoverned by legal principles. For example, a new product is still usually subject to existing tortious principles and product liability legislation, those selling it subject to consumer protection and competition law, and creators able to protect it under existing intellectual property legislation.[12] There is no need for legislators and judges to overreact to technological change. For example, a thief who steals a driverless smart car is still clearly in breach of section 154F of the *Crimes Act 1900* (NSW): the car's status as an eObject makes no difference to the fundamentals of the criminal offence.

In contrast, however, if the thief has an accident in the car causing injury or property damage, this may give rise to considerable uncertainty. Who will be liable for that damage: the thief; the owner; the manufacturer; and/or the third party developers of faulty software that allowed the car to be stolen in the first place? So in some cases there will be legitimate reasons for law to change as technology or the socio-technical landscape changes. One way this has been characterised is by Brownsword, as the challenge of 'regulatory connection' or 'disconnection'.[13] The concept of regulatory disconnection encompasses the discrepancies between existing law and other regulation created to order a previous socio-technical environment, which then require 'reconnection' with new actions, products and relationships made possible by new technologies.[14] This issue has also been characterised as a concern that law inherently has problems 'keeping up' with technological changes, sometimes referred to as the 'pacing problem'.[15]

This is not to say that an initial disconnection means that law will *always* be disconnected from socio-technical changes. Both legislatures and judges have in the distant and more recent past have acted to adapt or clarify the law to respond to technological change, such as:

---

[8] Roger Brownsword, *Rights, Regulation, and the Technological Revolution* (Oxford University Press 2008), Ch 6.
[9] Michael Kirby, 'The Fundamental Problem of Regulating Technology' (2009) 5 *The Indian Journal of Law and Technology* 1, 11.
[10] Ibid, 12.
[11] Bennett Moses, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target', above n 7, 9.
[12] Lyria Bennett Moses, 'Agents of Change: How the Law Copes with Technological Change' (2011) 20 *Griffith Law Review* 763, 768.
[13] Brownsword, above n 8. The challenges of regulatory connection and disconnection are discussed in detail in Chapter 6.
[14] Bennett Moses, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target', above n 7, 7.
[15] See eg Gary E Marchant, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer, 2011)

- in 1846, the NSW legislature created a new tortious suit of 'wrongful death' in response to the introduction of railways and other technologies of the industrial revolution; [16]

- in 2006, an Australian Federal Court judge clarified the common law for e-commerce transactions by expressly stating that a 'click' on a button on a website constituted 'a contract in writing signed by the parties'[17]; and

- in 2008, the Australian federal Parliament amended the definition of 'parent' to include non-biological parents where artificial conception technology is used.[18]

However, the speed of change and the timing of legal and other regulatory responses is important in successful reconnection. The need to address regulatory disconnection in a timely manner can be drawn out by examination of the potential effects of what has been labelled the 'Collingridge dilemma'. [19] The Collingridge dilemma recognises that in some cases:

> potential benefits of new technology are widely accepted before enough is known about future consequences or potential risks to regulate the technology from the outset, while by the time enough is known about the consequences and possible harms to enable regulating it, vested interests in the success of technology are so entrenched that any regulatory effort will be expensive, dramatic and resisted.[20]

However, the possible negative results of the Collingridge dilemma may dictate a need to respond to technologies as they emerge, and even before they come into existence or into commercial use. Once a technology has been fully developed, there is usually a strong incentive to resist any regulatory change, due mainly to the expense of changing technological design. Therefore, in some cases it may make sense to implement new laws before the technology is fully developed and/or the risks are fully known.**[21]** The speed of change reflected by the number of eObjects currently in commercial use and in advanced prototype[22] means that the challenges posed by the Collingridge dilemma are real and immediate.

---

[16] *Fatal Accidents Act (1846) 9 & 10 Vict c 93* (NSW) See Barbara Macdonald, 'Legislative Intervention in the Law of Negligence: The Common Law, Statutory Interpretation and Tort Reform in Australia ' (2005) 27(3) *Sydney Law Review* 443, 447-8.

[17] *eBay International AG v Creative Festival Entertainment Pty Limited* (2006) eBay International AG v Creative Festival Entertainment Pty Limited [2006] FCA 1768 , Rares J, 49. See further Kayleen Manwaring, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the U.S. and the U.K' (2011) 5(1) *Studies in Ethics, Law, and Technology* Article 4

[18] *Family Law Act 1975* (Cth), s60H.

[19]Bennett Moses, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target', above n 7, 8; Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge University Press 2012), 132. Collingridge himself described it as the 'dilemma of social control', David Collingridge, *The social control of technology* (Pinter 1980), 11.

[20] Morag Goodwin, 'Introduction: A Dimensions Approach to Technology Regulation' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing, 2010) 1, 2.

[21] Bennett Moses, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target', above n 7, 8.

[22] In 2011, Cisco predicted 50 billion devices will be connected to the Internet by 2020 (David Evans, '*The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper, April 2011' (2011)); more recently Gartner gave a more conservative estimate of 25 billion by 2020 (Gartner, 'Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015' (2014) <http://www.gartner.com/newsroom/id/2905717>).

In order to answer the question posed in the first paragraph in Part 2.2, this paper adopts the approach proposed by Bennett Moses in 2007.[23] Bennett Moses classifies problems that might arise out of a failure of regulatory connection in the context of socio-technical change into four categories:

(1) there may be a need to create special rules designed to ban, restrict, encourage, or co-ordinate use of a new technology; [**'new harms or benefits'**]

(2) there may be a need to clarify how existing laws apply to new artefacts, activities, and relationships, particularly where there is: '[a] uncertainty as to how a new activity, entity, or relationship will be classified; [b] uncertainty where a new activity, entity, or relationship fits into more than one category, so as to become subject to different and conflicting rules; [c] uncertainty in the context of conflicts of laws; and [d] uncertainty where an existing category becomes ambiguous in light of new forms of conduct'[24] [**'uncertainty'**]

(3) the scope of existing legal rules may be inappropriate in the context of new technologies; [**'under- or over-inclusiveness'**] and

(4) existing legal rules may become obsolete, where (a) the conduct regulated is no longer undertaken, or (b) the underlying facts have changed which means the rule is no longer justified, or (c) where the rule has become 'prohibitively difficult to enforce'[25]; [**'obsolescence'**][26]

Bennett Moses' approach is helpful particularly because it also recognises that some changes in technology will not give rise to regulatory disconnection, and even those which do to some extent will not create problems in all of the above four categories.[27] This approach also actively discourages any assumptions that just because a technology is new, it automatically generates uncertainty or a need for new rules.[28]

So how do we discover whether one or more of these types of problems arises in the case of particular eObjects? How do we best approach a review of existing laws to examine if there is a need for new legal rules to manage new risks or to encourage new behaviours, or if there exist legal rules which are obsolete, under or over-inclusive, or are uncertain?

Koops, in his 2010 attempt to map the field of technology regulation research, placed particular importance on the dimension of 'innovation' and the fact that non-innovative technologies are more likely to operate within existing regulatory frameworks than 'radically new technologies'. [29] However, he also explains that 'innovation' is not confined to

---

[23] Bennett Moses, 'Recurring dilemmas: the law's race to keep up with technological change', above n 2.
[24] Ibid, 269.
[25] Ibid, 268. The difficulties of enforcement in a world with eObjects is extensively discussed in Mireille Hildebrandt's work on 'ambient law'. See eg Mireille Hildebrandt, 'A Vision of Ambient Law' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, 2008) ; and Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) *Modern Law Review* 428.
[26] Bennett Moses, 'Recurring dilemmas: the law's race to keep up with technological change', above n 2, 285.
[27] Ibid, 246.
[28] Ibid, 252.
[29] Bert-Jaap Koops, 'Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing, 2010) 309-324, 313.

technologies that did not exist previously, but includes technologies which may have existed for some time, but where some form of change in the socio-technical environment has led to them becoming far more widely used. He argues that '[i]t is far from rare that a change in the scale of a technology gives rise to significant regulatory questions'. [30] Therefore, innovation can be seen when an 'old' technology becomes significantly more popular, or is re-purposed to achieve different outcomes.

It is useful then to examine the innovations contained within or around eObjects to see where problems falling into one or more of Bennett Moses' categories will most likely arise. Although some of the technology comprised in eObjects, such as Internet connectivity, may not be 'radically new', when compared with other innovations such as cloning or nanotechnology, a search for innovation should not be narrowly circumscribed to mere technical advances. For example, it is part of the very nature of the 'third wave' that many more 'things', or eObjects, will be connected to the Internet (or other internetworks) than previously. A change in scale this significant is likely to cause social change, which in itself may give rise to legal problems.

This section has identified the types of legal problems that might arise as a result of socio-technical change brought on by the development of eObjects. The categorisation of legal problems is important because it assists in ensuring that any legal problems identified are specific and defined, and reduce the likelihood that there is an overreaction to socio-technical change. This paper does not attempt to provide solutions to the legal problems identified. However the analysis and categorisation approach outlined by Bennett Moses can also be a useful analytic tool in research focussing on solutions. Precise categorisation helps to ensure that legal responses focus on a specific defined harm to protect against, or a benefit to encourage. But its use also allows successful solutions applied in particular areas to be considered for application across other areas. Where the essential nature of the problems are 'the same', such as under-inclusiveness or uncertainty, then solutions for one specific problem may well be the basis for solutions to other problems.

The next section illustrates how this categorisation of legal problems, in combination with an examination of the attributes of the technology under examination, can assist in a legal analysis of the socio-technical change brought about by the introduction of and growth in scale of the use of eObjects. It will do so by discussing some of the critical innovations contained in eObjects. Those innovations will be examined in order to develop a number of sample analyses of new things, activities and relationships arising out of eObjects, and the possibility that legal problems may arise out of these aspects of socio-technical change. One or more examples of instances that give rise or are likely to give rise to specific legal problems will then be discussed in detail. The emphasis is on Australian law, but examples from other jurisdictions are also used to illustrate the breadth of legal problems that may arise.

3 Innovations and legal problems

> What is really different about mobile computing? The computers are smaller and bits travel by wireless rather than Ethernet. How can this possibly make any difference? Isn't a mobile

[30] Ibid, 314.

> system merely a special case of a distributed system? Are there any new and deep issues to be investigated, or is mobile computing just the latest fad?[31]

Although Satyanarayanan asked this question about mobile computing, the same questions can be asked generally about the broader range of technologies encompassed within eObjects. This section of the paper will discuss socio-technical change arising out of some important innovations within eObjects. These innovations are not confined to developments in technical features, but also to changes in when and how the technologies are used.

As discussed in Part 2.2, in innovations (based on concepts not only of 'newness' but in changes of scale or purpose) lie some of the likely places for legal researchers to look for legal problems. These innovations – both technical and functional - have given rise to significant changes in how people use and interact with information technologies. However, it is important to remember, especially considering the large amount of marketing hype that exists regarding the potential of eObjects, that many innovations have 'side effects' that are not beneficial. Putting computers where no computers have previously existed creates technical problems that need to be overcome, act as constraints on performance or function, or provide affordances which may be beneficial to the creator but a disbenefit to the people being acted upon by the technology (for example sensor technologies that allow for collection of large amounts of personal information). Detriment to users may also arise when the law applies more restrictively to an activity that is carried out via an eObject as opposed to the same activity carried out using non-innovative technologies. Detriment to providers and others may also arise when technologies are used in ways not contemplated by their designers, while providing a countervailing benefit to the innovating users[32].

The particular innovations listed below have been chosen to illustrate the diversity of the legal problems that might arise in relation to eObjects. They have been identified with the use of Manwaring and Clarke's attributes framework identified in Part 2.1 and the Appendix. The innovations identified are illustrative, not comprehensive, and there are many more that could provide useful subjects for further research. These innovations include:

- increased **volatility** and **vulnerability** of computers and computing resources (see 3.1 and 3.2);
- the reintroduction of physical world concerns into cyberspace, particularly where the physical world affects and is affected by eObjects with attributes such as **vulnerability** and **active capacity** (see 3.3),
- the effect of the **mobility** of eObjects (see 3.4); and
- the **adaptability** of eObjects to the context surrounding them, particularly when combined with **geo-locatability** and **prevalence** (see 3.5);
- the different levels of **implicit human computer interaction**, particularly where it leads to reduced visibility of the device (see 3.6); and

---

[31] Mahadev Satyanarayanan, 'Fundamental challenges in mobile computing' (Pt ACM) (1996) *Principles of distributed computing: Proceedings of the fifteenth annual ACM symposium* 1, 1.

[32] '[T]he street finds its own uses for things' William Gibson, 'Burning Chrome (short story)', *Burning Chrome* (Harper Collins, 1995) One obvious example of this is the common practice of 'jailbreaking' of iOS, the operating system on iPhones and related devices, in order to install applications that are not available in the Apple App Store, or are more expensive than alternatives. See http://lifehacker.com/5781437/how-to-get-the-most-out-of-your-jailbroken-ios-device .

- the increased use of **autonomous or semi-autonomous** devices (see 3.7).

This list show that it is not only the attributes themselves, but also the relationships between them, which give rise to significant innovations in the way human beings interact with the technologies. These innovations in turn can raise questions about how these interactions are and should be regulated. One illustration can be drawn from the interaction of the characteristics of mobility, adaptability and prevalence. **Mobility** and **prevalence** of portable smart devices containing sensors, and the mobility of users interacting with smart environments with embedded sensors and communication links, mean that the places at which data might be captured have increased exponentially. The use of context-aware devices means that a particular action by a user actually generates more data about that user: where, when, how (and the list goes on). This all means that there is a lot more data being captured, much of which is stored, mined, manipulated and disclosed to third parties, and the nature of the data may potentially be more intimate[33] than that able to be collected previously.

It is not therefore surprising that most of the legal literature discussing eObjects concentrates on the privacy and data protection[34] implications. This is due to the ready availability of this potentially vast store of data about individuals, their lives, and their preferences, and in particular the inadequacy of existing laws and security systems to protect individuals. However, legal problems that may arise from the collection, storage and distribution of large amounts of data made possible by eObjects are unlikely to be confined to these areas. For example, Walker Smith contends that the increasing amount of information available to sellers about the way their customers use their products is set to increase product liability claims as the nature of foreseeability of harm changes.[35]

Technical innovations found in eObjects are not the only innovations of relevance. How the technology is operationalised, applied and used in a functional sense is also important. The nature of the interaction between a user and a desktop computer is different to that of a user and a smartphone, and different again to that of a person driving past a traffic sensor embedded in a stop sign. The differences are not just ones of overall design and functionality, but also of agency: that is, who or what is initiating and controlling the interaction.[36] Also, individual attributes may not be the most relevant ones, as the interaction between attributes may give rise to the most interesting legal issues.

3.1 Volatility of resources

Increased **volatility** of eObjects, and the systems in which they participate, may have harmful side effects. However, the disbenefits of these attributes are not uniform.

---

[33] Guido Noto La Diega and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016' (2016) <http://ssrn.com/abstract=2725913>.

[34] Note that these two terms are distinct, although they can be overlapping. For a discussion of the distinction, see for example R. Gellert and S. Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) *Computer Law & Security Review* 522. Others have further broken down the distinction into distinct 'dimensions' (eg Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms (last updated 21 October 2013)' <http://www.rogerclarke.com/DV/Intro.html#Mis>. or 'types' (eg Rachel L Finn, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth et al (eds), *European Data Protection: Coming of Age* (Springer, 2013) 3-32)

[35] Bryant Walker Smith, 'Proximity-Driven Liability' [1777] (2013-2014) 102 (6) *Georgetown Law Journal* 1777.

[36] Mireille Hildebrandt, *Smart technologies and the end(s) of law : novel entanglements of law and technology* (Edward Elgar Publishing 2015).

Depending on the type of device architecture, these particular constraints can operate weakly, strongly, or somewhere in between.

Satyanarayanan was among the first to outline what he considered the major 'constraints of mobility', which differentiated first mobile and then pervasive computing from other forms of distributed computing.[37] According to Satyanarayanan, smart devices will always be 'resource-poor' in relation to conventional desktop computing, in particular in relation to processing and network speed, memory and storage. He attributes this restriction on resources to considerations of 'weight, power, size and ergonomics'.[38]

Coulouris, writing 15 years later, essentially agreed with Satyanarayanan as to these constraints, but conflated them within his concept of 'volatility'. Volatility is the key factor by which he differentiates eObjects and the systems in which they participate from the original model of Internet-based distributed computing (desktop personal computers with mostly wired access to the Internet). Volatility is defined as when 'the set of users, devices and software components in any given environment is liable to change frequently'.[39] These volatility constraints manifest themselves in the different types of connections, energy sources and processing power utilised by smart devices.[40] In particular, connectivity for devices using wireless networks (whether the device is mobile or embedded) is usually more variable in relation to bandwidth, latency and reliability.

However, while the constraints of mobility are real and continuing,[41] they do not necessarily operate in the same way for all smart devices. For example, for small single- or limited-purpose devices, such as sensors in a thermostat system, poverty of processing power may well be a given. However, this must be contrasted with the more sophisticated technology available in modern smartphones. Advances in miniaturisation and other technologies have granted access to processing power, memory and storage for these multi-function devices to an extent that was well beyond the capacity of even desktop computing only a few years ago. It may always be possible to build a faster, more powerful desktop. But for many applications and many users, the difference in speed and processing power may not have an appreciable effect on the user.

The converse may well be true of access to a power source. Some low-power sensors may have access to what is effectively unlimited power for their lifetime, as they draw what little they need from energy harvesting devices, such as solar cells or piezoelectric materials (which harvest energy from motion).[42] Other smart devices, such as smart cards, obtain the minimal power supply needed for their functions from other parts of the smart system, for example a card reader. However, access to a power source is still a significant problem for

---

[37] Satyanarayanan, above n 31; Mahadev Satyanarayanan, 'Pervasive computing: vision and challenges' (2001) 8(4) *IEEE Personal Communications* 10. Satyanarayanan's papers are still widely quoted by modern computer scientists eg Frank Adelstein et al, *Fundamentals of mobile and pervasive computing* (McGraw-Hill 2005), 5; Stefan Poslad, *Ubiquitous computing: smart devices, environment and interaction* (John Wiley & Sons Ltd 2009); George F Coulouris et al, *Distributed systems : concepts and design* (Addison-Wesley (Pearson Education) 2012).

[38] Satyanarayanan, 'Fundamental challenges in mobile computing', above n 31.

[39] Coulouris et al, above n 37, 817.

[40] ibid, Ch 19.

[41] Matt Smith, 'Why your smartphone won't be your next PC' (2013) *3 August 2013 Digital Trends* <http://www.digitaltrends.com/computing/why-your-smartphone-wont-be-your-next-pc/#!US6P1>.

[42] Eg solar-powered calculators, or Midé's Volture Piezoelectric Vibration Energy Harvesters (commercially available), http://www.mide.com/products/volture/piezoelectric-vibration-energy-harvesters.php.

more complex devices with greater computational power. Almost anyone with a smartphone has at one time or other lamented over the speed at which his or her battery has been drained. While there have been some recent advances in energy harvesting technology that may eventually lead to 'chargeless' mobile phones,[43] any commercial application of this is some years away. As a result, many eObjects still need to be designed to minimise power consumption, with corresponding negative effects on processing power and speed.

There are significant liability issues which might arise here, especially in relation to the failure of eObjects used in healthcare, such as wirelessly-controlled insulin pumps and pacemakers, which can cause serious physical personal harm. It is possible that litigation against software and hardware providers will increase as a result of the widespread use of eObjects. Many of the issues likely to be raised in such litigation may well already be 'covered' by the existing laws of tort and contract. However, developers, suppliers, investors and consumers may be uncertain about how the law will apply to the specific facts surrounding their development, use and sale of particular eObjects. Entities throughout the provider network may well also be uncertain as to whether their insurance contracts may respond to such claims. Even if they do, the likelihood of higher insurance premiums for software companies, along the lines of the professional health care worker who pays out many thousands a year in public liability insurance, is more probable than not. And this may lead to further uncertainty about maintaining profitability, and therefore stifle investment in innovative health technologies.

Judges interpreting the common law of tort and contract may well, left to themselves and the litigation system, make it clear how the law applies in new factual situations. However, the litigation process is not a speedy one. Therefore, business and society may legitimately expect Parliament or other holders of regulatory power to act, where the uncertainty is so significant as to negatively affect the way the technology is funded, developed and used. The Collingridge dilemma may well have an important part to play here. If assumptions are made about the way judges will determine liability in a particular circumstance, development of the technology may follow a certain path in order to avoid unwanted consequences. This path may be a sub-optimal one from an economic and/or social viewpoint, and unnecessarily so if the assumptions are proven incorrect by the cases which are eventually decided.

3.2 Vulnerability and security

Very early on, Satyanarayanan identified that eObjects are in many cases inherently less secure.[44] This particularly applies to mobile hardware, which can be stolen or damaged more easily. For example, a mobile phone, or a wearable electronic device such as a fitness tracker,[45] is more vulnerable to theft than a desktop computer. However, this issue is not

[43] Eg Y. Mao et al, 'Sponge-Like Piezoelectric Polymer Films for Scalable and Integratable Nanogenerators and Self-Powered Electronic Systems' (2014) 4(7) *Advanced Energy Materials* . This paper describes their work in developing a mesoporous piezoelectric nanogenerator.

[44] Satyanarayanan, 'Pervasive computing: vision and challenges', above n 31.

[45] Eg the Fitbit Flex wristband (commercially available) which contains sensors which tracks physical activity and sleep patterns, and then syncs with smartphones or conventional computers to create a data profile. See www.fitbit.com.

confined to the simplicity of stealing a small, light and robust machine as supposed to a large, heavy and fragile one.

More recently, significant evidence is emerging that some eObjects and the systems in which they are used may well be more prone than conventional connected computers not just to physical interference but also to remote attacks. This is due to the existence of particular security vulnerabilities in the eObjects themselves and the systems in which they participate. These vulnerabilities include: insecure network services; insecure interfaces; insecure software and firmware; lack of encryption; insufficient authentication and authorisation; insufficient security configurability; the storage of personal data; and the lack of physical safeguards.[46]

Remote attacks can include the remote operation of the eObject without the permission of the local user ('hacking') and/or the delivery of malicious software ('malware'). [47] Examples of consequences of these types of attacks include:

- the disclosure of sensitive data (eg passwords, personal information) for use by the attacker, or exposure to the outside world;
- modification of data for personal gain (including repudiation);
- allowing the attacker to act on behalf of the user ('spoofing' or 'masquerading');
- instigating denial of service (DoS), and distributed DoS attacks;
- attacking other eObjects or conventional computers; and
- causing physical harm to or destruction of the eObject, surrounding objects and/or people.[48]

Commentators attribute the amount of security problems with these devices to:

- the inexperience of (and possible disinterest by) consumer goods manufacturers in security issues (as compared to specialist IT manufacturers);
- the small size of some devices may not support the processing power needed for strong security measures such as encryption; and
- most of the devices are not designed to accommodate software updates, making security patches unworkable. [49]

Security researchers have recently proven the ease of remote attacks on consumer devices such as the aforementioned fitness trackers,[50] healthcare devices such as insulin pumps[51]

---

[46] This is a consolidated list adapted from the Open Web Application Security Project, *Top 10 IoT Vulnerabilities (2014) Project* Open Web Application Security Project Wiki <https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29>

[47] Roger Clarke and Alana Maurushat, 'Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity?' (2007) 18 *Journal of Law, Information & Science* 8, 35.

[48] This is a consolidated list adapted from Cloud Security Alliance Mobile Working Group, *Security Guidance for Early Adopters of the Internet of Things (IoT) (April 2015)* (2015)

[49] Peppet, above n 4; Bruce Schneier, 'The Internet of Things is Wildly Insecure - and often Unpatchable' (2014) *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/>.

[50] Eg Fitbit, Mahmudur Rahman, Bogdan Carbunar and Madhusudan Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) *arXiv:1304.5672 [cs.CR]* ; Mario Ballano Barcena, Candid Wueest and Hon Lau, Symantec Security Response Report, 11 August 2014, *How safe is your quantified self?* .

and heart defibrillators,[52] domestic appliances such as Internet-connected kettles[53] and smart fridges,[54] and even baby monitors[55] and childrens' toys.[56] The security implications and the damage security exploits can cause already extends past intimately personal devices and their potential harm to one person. In the last five years, security researchers have successfully managed to exploit flaws in some cars' Internet-connected internal systems in order to wirelessly control cars' locks, brakes, steering and transmission. Hacks have also included remote tracking of the cars' physical locations.[57] General Motors took nearly five years to fully protect its cars against an exploit identified by security researchers in 2010.[58] This sluggish response by General Motors gives weight to Peppet's concerns about the capability of consumer goods manufacturers – even highly sophisticated ones with significant resources – to deal with security problems in an efficient and timely way.

In most jurisdictions with developed legal systems, detailed rules about car safety exist. However, depending on drafting, these may well be inadequate to deal with the increased ability of third parties to cause harm by malicious remote control of a heavy motor vehicle at speed. The harm itself is not 'new'. Personal injury and property damage resulting from the impact of a vehicle has been occurring since the first wheeled vehicles were invented, and these harms are already regulated under both tort law and specific motor vehicle legislation. The legal problem here is most likely to be one of 'under-inclusiveness'. Of course, unauthorised remote intrusion is already a criminal offence in many jurisdictions,[59] but considering the myriad of approaches and definitions used by drafters, it is worth re-examining whether this particular type of intrusion will automatically be covered under existing legislation. For example, the Western Australian legislation confines the offence to unlawful access to password-protected computer systems.[60] An individual user buying a

---

[51] Jordan Robertson, 'Insulin pumps, monitors vulnerable to hacking' (Pt Fairfax) (2011) *Sydney Morning Herald* <http://news.smh.com.au/breaking-news-technology/insulin-pumps-monitors-vulnerable-to-hacking-20110804-1idfn.html>.

[52] 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, blood refrigeration units and CT scans. See Kim Zetter, 'Medical devices that are vulnerable to life-threatening hacks' (2015) *Wired.com* <http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x>.

[53] Catalin Cimpanu, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks Across London' (2015) *Softpedia (20 October 2015)* <http://news.softpedia.com/news/insecure-internet-connected-kettles-help-researchers-crack-wifi-networks-across-london-494895.shtml>.

[54] Ibid.

[55] Kashmir Hill, 'Crib Cams: Watch out new parents - internet-connected baby monitors are easy to hack' (2015) *Fusion.net (3 Sep 2015)* <http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/>.

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

[57] 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/> ; Stephen Checkoway et al, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' in D Wagner (ed), *Proceedings of USENIX Security 2011, Aug 2011* (USENIX, 2011) ; Nick Bilton, 'Bits Blog: Disruptions: As New Targets for Hackers, Your Car and Your House', *New York Times*, 11 August 2013 <http://bits.blogs.nytimes.com/2013/08/11/taking-over-cars-and-homes-remotely/?_r=0>

[58] Andy Greenberg, 'GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars', *Wired*, 10 Sep 2015 <http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/>

[59] Eg the US: *18 US Code § 1030 - Fraud and related activity in connection with computers*, , and under the State Codes (http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx); Australia: *Criminal Code Act 1995* (Cth), Part 10.7, *Crimes Act 1958* (Vic), ss 247A-247I, *Crimes Act 1900* (NSW), Pt 6 ss 308 – 308I, *Summary Offences Act 1953* (SA), s 44, *Criminal Code 2002* (ACT), ss 412-421, *Criminal Code Compilation Act 1913* (WA), s 440A, *Criminal Code 1899* (Qld), s 408E, *Criminal Code Act 1924* (Tas), Schedule 1, ss 257A-F; *Computer Misuse Act 1990* (UK)

[60] *Criminal Code Compilation Act 1913* (WA), s 440A.

cheap consumer eObject has no guarantee that their device is actually password-protected, and usually no capacity to implement that protection for themselves.

Even rules that are not under-inclusive – that is, they cover all relevant conduct – may nevertheless be ineffective if they cannot be enforced effectively. A hacker may well be in breach of a 'no access without lawful excuse' rule, but many hackers are notoriously difficult to find and enforce criminal penalties against, especially as they could be anywhere on the planet[61]. To ensure the safety of the public, it would make more sense to ensure that car manufacturers should be expected to take some responsibility for security flaws in their systems. However, manufacturers' most likely response in the absence of regulatory intervention will be an attempt to exclude tortious and other liability for security breaches by clauses inserted in sale contracts.

Software contracts are already notorious for the breadth of their exclusion clauses,[62] and it is naïve to assume that car manufacturers' legal advisors will not adopt a similarly broad approach. Some premium car manufacturers may also of course improve security features in order to increase brand reputation among consumers; but not all, and not all to the same extent. Although car manufacturers are already required to manufacture cars to quite strict (and detailed) safety standards that are enforced by legislation, these standards generally do not include security standards for Internet-connected systems. In the US, at least, the existing safety standards are not considered sufficient to cover this type of intrusion. On 21 July 2015, a Bill directing government bodies[63] to promulgate regulatory standards for car cybersecurity (and data protection) was introduced into the US Senate.[64]

3.3 Vulnerability and active capacity

The discussion above highlights that one of the key consequences of technological developments related to eObjects is the re-emergence of physical spaces and places as an important concept in information technology.[65] When scholars and others talk about cyberspace, they tend to concentrate on its intangible aspects, its status as a mass 'consensus-hallucination'[66] rather than a space in which actions are carried out. Cyberspace has traditionally been conceived as a world without boundaries or physicality, or even a positive denial of a physical place. [67] The role of the physical environment in conventional distributed systems is usually limited to acting as a conduit for power and communications, and as a repository for data storage and processing units.[68] However, the physical location of an embedded smart device – or, in the case of a mobile device, its ability to move quickly and easily in space between physical locations without losing functionality - forms an

---

[61] Or even in low Earth orbit, considering even the International Space Station has an Internet connection - http://www.tested.com/science/space/449539-how-fast-isss-internet-and-other-space-questions-answered/

[62] Marc Goodman, *Future crimes : everything is connected, everyone is vulnerable and what we can do about it* (Doubleday 2015), 7664-73 [Kindle edn location].

[63] National Highway Traffic Safety Administration (NHTSA) and the Federal Trade Commission (FTC).

[64] *SPY Car Act of 2015, S 1806, 114th Congress (2015)* .

[65] Paul Dourish and Genevieve Bell, *Divining a digital future: mess and mythology in ubiquitous computing* (MIT Press 2011).

[66] Gibson, above n 32, 196-7.

[67] Roger Clarke, 'Paradise gained, paradise re-lost: how the Internet is being changed from a means of liberation to a tool of authoritarianism' (2001) 18(August 2001) *Mots Pluriels*

[68] Poslad, above n 37, 8.

essential part of its nature, and is inextricably linked to its use by humans. [69] So when we move from a cyberspace 'no-place' to a confrontation with the limitations of the physical world, this gives rise to certain questions about how the law will and should act in particular situations.

One of the most obvious implications of the physicality of devices and systems in eObjects is in the security concerns outlined in section 3.2, particularly in the example of car hacking. A desktop computer is a large and heavy object, but remote hackers have not been generally able to pick one up and throw it across a room. Within the world of eObjects, a potentially dangerous innovation lies in the interaction between the eObject attributes of **vulnerability** and **mobility** – a malicious hacker can remotely control a one-and-a-half tonne piece of metal travelling at 100km/hour and use it to injure people and property. The relevant legal problem of 'under-inclusiveness' is discussed in Part 2.2 above.

The greatly desired 'smart home' potentially brings with it similar practical problems, although mobility is not the attribute interacting with vulnerability here, but rather **active capacity**, the ability of eObjects to interact with the physical world. For example, you may own a smart house, and have just bought an Internet-enabled designer lamp for both its aesthetic appeal and its advertised compatibility with your particular smart house system. However, unbeknownst to you, the lamp contains a security vulnerability that allows a rogue to hack into your smart house system, turn off the sprinklers and the fire alarm, and turn on the stovetop. Consequently, the house burns down. The rogue cannot be tracked down, so a search for liability will begin with the service providers relating to your smart house. A similar problem may arise here with 'under-inclusiveness' around safety and security standards as applies to car hacking (see section 3.2). However, in the smart home example there are likely to be many more suppliers and manufacturers providing eObjects and their related services. Therefore, a new set of uncertainties arises around concepts of causation and liability in contract, in tort and under consumer protection laws.

For example, in Australia, consumer goods are sold subject to a guarantee of 'acceptable quality', under section 54 of the *Australian Consumer Law* (ACL)[70]. A lamp that does not turn on is obviously not of acceptable quality, but what about an Internet-connected lamp with a security vulnerability? However, in a common law system like Australia's, until a judge answers the specific question as to on which side of the 'acceptable quality' line security vulnerabilities lie, consumers, suppliers and insurance companies will not know how the law applies in this situation. And, as factual situations shift, this uncertainty will continue. The position may be somewhat clearer in the United States. The Federal Trade Commission (FTC) has brought a number of enforcement actions against companies relating to inadequate cybersecurity practices under section 5 of the *Federal Trade Commission Act,*[71] which prohibits 'unfair or deceptive acts or practices in or affecting commerce'.

---

[69] Dourish and Bell, above n 65, 109.

[70] *Competition and Consumer Act 2010* (Cth), Australian Consumer Law, Schedule 2, Part 3-2.

[71] *15 US Code § 45 - Unfair methods of competition unlawful; prevention by Commission* . A list of FTC enforcement actions on Data Security can be found on the FTC website at https://www.ftc.gov/tips-advice/business-center/legal-resources (select 'Data Security' from the Topic menu to filter.) The FTC has most recently settled a case against ASUS relating to security vulnerabilities in home routers and Jessica Rich, Director of the FTC's Bureau of Consumer Protection stated 'The Internet of Things is growing by leaps and bounds, with millions of consumers connecting smart devices to their home networks. Routers play a key role in securing those home networks, so it's critical that companies like ASUS put reasonable security in place to protect consumers and their personal information. Federal Trade Commission, 'ASUS Settles FTC

However, it has only recently been confirmed by the US Court of Appeals that inappropriate cybersecurity practices could amount to 'unfair conduct' under section 5, in an action by the FTC against a hotel chain whose customer data had been subject to three data breaches in two years.[72]

The consequences of this uncertainty outside of judicial decisions are however somewhat predictable. Consumer guarantees of acceptable quality cannot be excluded by contract. However, specific disclosures by a supplier can remove the protection of this guarantee.[73] Knowing this, and once aware of the potential liability, suppliers will (particularly to maintain insurance coverage) most likely amend their point of sale material and/or contractual boilerplate to include a broad 'disclosure', which will have the same effect as an exclusion clause. An attempt by consumers to shift blame to the smart home system supplier for a failure to block security exploits at the point of interconnection will most likely face the same contractual roadblock.

3.4 Mobility

One common attribute of eObjects is **mobility**. This attribute, along with a closely related attribute, **portability** (where the eObject itself can be moved but is not designed to communicate while doing so) mean that transactions and interactions with people, with businesses, with information and with the devices themselves are carried out in different ways and in different places, than those transacted under the desktop model. One important consequence is that the nature of the information flow around the transactions can also be substantially different from that found in traditional computing, particularly traditional e-commerce. In particular, the widespread use of sensor technologies makes it likely that a greater quantity of data can and will be collected by eObjects (whether they are mobile or whether the people interacting with them are). This increase in data collection is occurring 'alongside the rapid deployment of ancillary technologies, equipment, and services to aggregate information and make it widely accessible'.[74]

This greater availability of data can lead to issues around privacy, data protection and the legitimacy of surveillance; but it can also have benefits for individuals. For example, Peppet points out that consumers can now access a greater availability of information about products while in-store, including review sites that specifically raise issue with onerous contract terms, as well as the quality of the product and ongoing support services. He argues that consumers can therefore more easily work out what firms offer the best deal, over and above price considerations.[75]

The 'constraints of mobility' identified by Satyanarayanan[76] also mean that in some cases different technical or business solutions are implemented for activities that are functionally

---

Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk') <https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>

[72] *Federal Trade Commission v Wyndham Worldwide Corporation* [2015] Federal Trade Commission v Wyndham Worldwide Corp, No 14-3514, F 3d (Aug 24, 2015))

[73] *Competition and Consumer Act 2010* (Cth), Australian Consumer Law, Schedule 2, ss54(2)-(4).

[74] Kevin Werbach, 'Sensors and Sensibilities' [2321] (2007) 28(5) *Cardozo L. Rev.* 2321, 2338. See also the discussion in Uteck, above n 4, 41: '[w]hen mobility and digital information merge, the nature of the information changes'.

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

[76] Satyanarayanan, 'Fundamental challenges in mobile computing', above n 31.

the same to a user whether undertaken on a desktop or via an eObject. The solutions proposed to overcome a problem with, or meet an opportunity for, mobility may well have different legal implications, even though the difference cannot be seen or is considered irrelevant by the end user. One particular example of this has already been raised in formal litigation. In Australia, s111 of the Copyright Act 1968 allows for copying of television shows for private use without breach of copyright (the 'time-shifting exception').

In *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd* [2012] FCAFC 59, however, an implementation of a time-shifting solution via mobile phones led to a breach of the Act. Telstra had entered into an exclusive deal with the AFL and the ARL for its mobile customers to view football matches on their mobile phones. Optus offered a competing service where its mobile users could record and play back football matches offered on free-to-air television on their mobile phones or other computers. The technical structure of the service offered by Optus involved:

- the interception of the television signal by Optus receivers;
- the making and storage of an individual copy (one for each user) on Optus servers; and
- access by the user when s/he wished to watch a particular show.

The making and storing of the copies by the service provider on their own server, rather than the user's device, would have been done (at least in part) in order to address the resource constraints of mobile phone hardware and Internet connectivity. In particular, the storage space required to copy large media files would soon overwhelm the capacity of most smartphones.

It is arguable that from the perspective of the individual user, this activity whether performed at home or on the move was the same, comprising the recording and playback of free-to-air television shows at a time that suited them. The trial judge agreed with this approach. However, the appellate court disagreed. The extent of the uncertainty raised by this issue here was highlighted by the fact that the trial judge's approach was similar to that adopted by appellate courts in the US and Singapore. The Full Federal Court in Australia preferred the approach of a Japanese appellate court, but not without controversy.[77] When the dispute first arose, it revealed a legal problem falling into Bennett Moses' 'uncertainty' category: that is, the uncertainty of the application of s111 to new ways of making copies of television programs for private use. The Full Court itself acknowledged the uncertainty in the questions raised in the appeal.[78] They also admitted that uncertainty continued to exist in relation to other technical solutions for time-shifting, which were not the subject of this litigation.[79]

---

[77] *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd* [2012] FCAFC 59 For a discussion of this case, see Rebecca Giblin, 'Stranded in the Technological Dark Ages: Implications of the Full Federal Court's decision in NRL v Optus' (2012) 35 *European Intellectual Property Review* 632 and Kayleen Manwaring, 'A shift in time saves no-one: mobile technologies and the NRL v Optus decision' [83] (2012) 5(No 1 & 2) *Journal of the Australasian Law Teachers Association* 83.

[78] *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd* [2012] FCAFC 59 at [9]: '[w]e have found the questions raised in the appeals to be of some difficulty and considerable uncertainty'.

[79] Ibid, [100]: 'We accept that different relationships and differing technologies may well yield different conclusions to the 'who makes the copy' question'.

In addition to the continuing uncertainties, the decision has raised a potential problem of 'under-inclusiveness', depending of course on the viewpoint of the person examining s111. However, a policy question remains. Is the interest that a private user has in being able to make copies for time-shifting purposes one that should be protected *notwithstanding* any third party technologies and third party services they employ?

The question of possible under-inclusiveness was addressed, in an indirect way, in the decision. The Full Federal Court explicitly recognised that technological neutrality was seen to be a desirable goal,[80] but did not believe that s111 as drafted operated to achieve this goal. The judges implied that if this goal was to be met, Parliament must act to amend the wording of s111. A 'liberal approach' to interpretation, such as that proposed by the law and technology theorist Cockfield,[81] may have allowed the judges to address the lack of protection of private users' interests. However, the judges refused to take this approach, based partially on an argument that there were 'conflicting interests and values'[82] to be taken into account, which in their opinion called for a legislative choice to be made, not a judicial one.

Of course, this interpretation by default ranked the interests of the copyright owners and their licensees above those of private users and technology innovators. The question remains for Parliament of whether this is the appropriate ranking to make? This dilemma of course does not just illustrate an example of 'under-inclusiveness', but also highlights the difficulties regulators must face in addressing such a legal problem. For in many, if not most, cases of socio-technical change leading to claims of under- (or indeed over-) inclusiveness, there will be a competition of interests. The competition will be between those of members the 'under-included' community, and those corporations, individuals or governments who receive an economic, social or other benefit from the status quo.

3.5 Adaptability, geo-locatability and prevalence

Adaptability and geo-locatability are closely related attributes of eObjects. Adaptability, also known as 'context-awareness', refers to the idea that an eObject can identify in real time some part of its user's context - who the user is, where she is, the environment through which she is moving, her habits and preferences – and it or the system in which it participates can reconfigure and adapt itself accordingly. The greater capabilities brought about by adaptability in technology, if realised to their full potential (and this is a big 'if'), will most likely bring about the greatest socio-technical changes related to eObjects.

In contrast, geo-locational technologies have been adopted in very many mobile eObjects. Within the traditional model of distributed information technologies, where a desktop is physically located has been, in most contexts, irrelevant,[83] as well as difficult to determine accurately. However, now eObjects are mobile, and more likely to be 'personal', that is, intimately associated with an individual. A person with a smartphone can be located (almost) anywhere at (almost) anytime. Geo-locatability is not only available to

---

[80] Ibid, [95].

[81] Arthur J. Cockfield, 'Towards a law and technology theory' (2004) 30(3) *Manitoba Law Journal* 383.

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

[83] There is at least one notable exception to this - 'geoblocking' (the practice of limiting access to content (particularly TV programs and movies) on the Internet based on your geographic location): Daniel Dionne, 'Explainer: what is geoblocking?' (2013) *The Conversation* <https://theconversation.com/explainer-what-is-geoblocking-13057>..

telecommunication carriers or government security agencies, but to everyday consumers using a cheap (or even free) app on their smartphones, such as 'Find my Friends' (Apple iOS) or Life360 (Android and Windows). However, it must be emphasised that the accuracy of such location tracking, whether consensual or imposed, is not always, or even often, particularly robust. Accuracy and reliability of common geo-locational technologies are heavily dependent on the device, the actual location techniques and the circumstances at the time that they are used.[84] Geo-locational data may also be obfuscated or falsified, for example to protect privacy or hide responsibility for criminal activity.[85] This is particularly important to remember when such technologies are presented as evidence in criminal trials.

The use of geo-locatability and adaptability attributes in the commercial sphere was early postulated by Kang and Cuff in 1996, through the development of their speculative description of a 'networked mall'.[86] This idea of a 'networked mall' has recently manifested itself in reality with the introduction of enterprise mobile marketing eObjects such as Apple's iBeacon (although the adaptability features are fairly unsophisticated at present). iBeacon and like products ('beacon implementations') marry precise geo-location targeting and context data (for example retail products within near proximity, purchase history and preferences, time of day). Beacon implementations use indoor positioning devices and systems with small low-power sensors[87] to track when subscribers carrying their mobile phones enter a particular physical space (such as a particular section of a department store). When a person is located in a particular place (for example the shoe aisle in a department store), this triggers an action by applications in the mobile phone, such as notifications as to nearby items which are then offered at a discount. Although the use of beacon technology is not yet widespread, in 2015 it had already been installed in some malls and has extended into other public spaces such as airports, baseball stadiums and museums. This technology is also currently being used or piloted by shopping centres, fast food, sporting, airline and pharmacy and other business enterprises.[88]

Beacon implementations rely on eObjects with access to personalised profiling data and with the potential to be programmed to act in accordance with copious research on how consumers actually make purchasing decisions. An average human shop assistant, at least when dealing with a new customer, is unlikely to have either the personal knowledge of the customer, or the aggregated knowledge of purchasing patterns, that can be contained in or associated with an eObject. The digitisation of commerce generally (mediated through

---

[84] Katina Michael and Roger Clarke, 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' (2013) 29 *Computer Law & Security Review* 216, 217-218.

[85] Roger Clarke, 'A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy (Draft of 16 August 2015)' <http://www.rogerclarke.com/DV/Biel15-DuDA.html#App3>.

[86] Jerry Kang and Dana Cuff, 'Pervasive Computing: Embedding the Public Sphere' (2005) 62 *Washington and Lee Law Review* 93, 121-145.

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

[88] Eg Macy's, McDonalds, Major League Baseball, Walgreens, Virgin Atlantic, Japan Airlines, American Airlines. Trips Reddy, '15 Companies From Airports to Retail Already Using Beacon Technology' (2014) <https://www.umbel.com/blog/mobile/15-companies-using-beacon-technology/>; James Wood, 'iBeacon: the Future of Content Marketing?' (2014)(7 October 2015) *B2B Marketing* <http://www.b2bmarketing.net/blog/posts/2014/02/17/ibeacon-future-content-marketing>.. Australian implementations have included Chatswood Chase shopping centre (http://www.bienalto.com/2014/09/ibeacon-pilot-at-chatswood-chase-reveals-a-data-rich-future-for-retailing/), Bendigo Marketplace (http://iproximity.net/smart-shopping-bendigo-marketplace-ibeacon-proximity-enabled-hellolocal-app/) and Tourism & Events Queensland (http://statements.qld.gov.au/Statement/2015/3/29/beacons-signal-new-way-for-visitors-to-explore-queensland).

conventional desktops and eObjects) may grant firms with large marketing budgets an enhanced ability to target consumers' cognitive biases and particular vulnerabilities and use that information to encourage consumers to make purchasing decisions in the firms' best interests, rather than in the consumers' own.[89] A further attribute of eObjects – **prevalence** – will come into play here, not just in terms of delivery of the message, but in collection of data. The uses of eObjects in e-commerce widen the reach of a marketer to a significant degree. As a result of all of these factors, commentators in the US[90] and Europe[91] have expressed concern that consumer protection law in their jurisdictions will not be broad enough to cope with the increased capacity of firms to collect intimate data and exploit it in ways where they have a high potential to persuade consumers into unwanted transactions.

This is also a potential concern for Australia. This type of taking advantage of consumer weaknesses can be sensibly categorised as some sort of 'unfair persuasion'[92], but the law in Australia does not recognise this as a general principle of prohibited conduct. The common law, and the Australian Consumer Law contained in Schedule 2 of the *Competition and Consumer Act 2010* (ACL) have some specific areas where consumers are protected from sellers preying on their vulnerabilities, but these are confined and it is not yet certain whether or not these new forms of conduct will actually be regulated under these provisions. For example, the ACL provisions on misleading or deceptive conduct[93] have previously placed considerable reliance on the existence of a misrepresentation.[94] While the High Court has recently made it clear that Australian law does **not** require an explicit or implied misrepresentation for section 18 of the ACL to apply, there is still a requirement that the plaintiff be led (or is likely to be led) into error.[95] What is currently uncertain is the scope of the definition of 'led into error', and how broadly judges will interpret this requirement. Where such techniques are used exclusively, the consumer will not be in receipt of incorrect or incomplete information as to any innate attribute of the goods or services. Rather, they are put in a situation where they are more likely to agree to buy them due to their own vulnerabilities, such as being offered a discount on conveniently located junk food at the end of a long day when their willpower is most likely to be at its lowest ebb.

ACL provisions on unsolicited consumer agreements[96] do not require any form of falsehood, but recognise the need for heightened protections where consumers are put in situations where they are at their most vulnerable. However, these provisions are confined to door-to-door and telemarketing sales, and the use of digital persuasive techniques will not fall under these protections. This is concerning in the light of psychological research that

[89] Ryan Calo, 'Digital Market Manipulation' (2014) 82(4) *George Washington Law Review* 995, 999, 1043-4.
[90] Ibid.
[91] 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)
[92] Calo, above n 89, 237.
[93] *Competition and Consumer Act 2010* (Cth), Australian Consumer Law, Part 2-1 Division 1, Schedule 2.
[94] For a discussion of the case law on this, see Alex Bruce, *Consumer Protection Law in Australia* (2nd edn, LexisNexis Butterworths 2014) 85-6.
[95] *Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Ltd* [2010] HCA 31 , [15]
[96] *Competition and Consumer Act 2010* (Cth), Schedule 2, Australian Consumer Law, Pt 3-2 Div 2.

indicates that people can and do respond to computer-delivered persuasive techniques in a similar way as they do with real people.[97]

Of course, it is not yet a given that Australian law **should** protect a consumer against these types of frailties. However, if this becomes the normative position, the ACL in its current state is definitely uncertain, and likely to be under-inclusive. The more general law prohibiting unconscionable conduct, both under statute and in equity, may be called into action by consumers. But this in itself will most likely lead to a problem of uncertainty, as judges have never yet had to deal with this combination of 'intense systematisation' and 'personalisation' of data[98], and will find little in the cases by way of precedent or even analogy.

3.6 Reduced visibility and human-computer interaction

From the beginning, Weiser and others have characterised ubiquitous computing as 'calm technology', or 'technology which disappears'.[99] Of course, many eObjects are still highly conspicuous, for example smartphones or 'phablets'.[100] For other eObjects however, particularly wearables or surveillance technologies, the computing power and/or data communication capabilities of the objects are unobtrusive to a greater or lesser degree. This lack of visibility potentially has consequences for the nature of human interaction with these types of technologies. Of course, this concept is already known within conventional distributed computing. Much of the interaction between the multiple machines and systems that are required to do mundane tasks, such as searching the Internet, is hidden from users, who to all intents and purposes appear to themselves to be interacting with one machine and one software application. However, the interactions are still there and tend to be intentional and purposeful, through the use of peripherals such as a keyboard, mouse, or touchpad.

However, advances in **implicit** (or at least **less obtrusive**) human computer interaction (both current and projected), mean that this level of purposeful interaction should not be taken for granted. Much of this technology is still in the research stage,[101] but some technologies have already matured to commercialisation. Networked sensors to manage lighting in commercial buildings are already mainstream.[102] Gesture-based command technology is common in the games market.[103] Wearable cameras with automated photo-taking functions, or 'lifeloggers' have also recently entered the consumer and healthcare

---

[97] B. J. Fogg, *Persuasive technology : using computers to change what we think and do* (Amsterdam ; Boston : Morgan Kaufmann Publishers 2003) cited in Calo, above n 89).
[98] Calo, above n 89, 1021.
[99] Mark Weiser, 'The Computer in the 21st Century' (Pt 1991) [94] (1991) *Scientific American* 94, 1; Mark Weiser and John Seely Brown, *The Coming Age of Calm Technology* (5 October 1996) <http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm>; Satyanarayanan, 'Pervasive computing: vision and challenges', above n 31. Poslad included this 'calm computing' concept as a sub-property of his iHCI core property classification.
[100] 'Phablets' – a portmanteau of 'phone' and 'tablet', referring to smartphones with large screens.
[101] For examples, see Rami Albatal et al (eds), *Shaping our digital lives* (2014) , Masaaki Kurosu (ed), *Towards Intelligent and Implicit Interaction* (Springer, 2013)
[102] Eg http://www.legrand.com.au/products/energy-management/sensors/scs-networked-sensors/
[103] Eg Microsoft's Kinect system, http://www.xbox.com/en-AU/Kinect .

markets,[104] following on from a longer history of use of body-mounted cameras by law enforcement agencies.[105]

If visibility of the technology used to mediate consumer contracts does decrease significantly, this may well give rise to contractual and consumer issues. It is no new thing to have contracts mediated through technology. However, interesting questions can be asked as to whether the absence of particular forms of contractual processes changes the dynamic of the relationship between contracting parties. If the dynamic does change, how will judges interpreting the existing common law and legislation deal with this? For example, what issues might arise around enforceability of contracts formed through interaction with 'invisible' devices? How is consent to terms and conditions indicated, and proved, in the absence of point-and-click? How will a judge interpret the requirements of notice for onerous clauses in environments where such notice can only practically be provided a step, or number of steps, removed from the purchase and use of a relevant item?

One of the greatest impacts of developments in implicit human-computer interaction is of course its potential impact on privacy and data protection. If the level of implicit human computer interaction built into an eObject, or a series of eObjects, is such that a person does not know you are interacting with a device or devices that gathers data and transmits it to others, how can that person prohibit or limit the use of the information gathered as a result of that interaction?

When personal information is collected from individuals by firms and government bodies, privacy policies are required in many jurisdictions, such as Australia, the US and Europe. For example, the Australian Privacy Principles (discussed in more detail below) require Australian government bodies and commercial organisations to have a privacy policy. A privacy policy is easy to implement as part of conventional computing via a link on a website to a detailed privacy policy and an 'I agree' button. Most companies (in jurisdictions such as the US, Australia and Canada at least) will have a privacy policy and display it on their website, and will, theoretically, be subject to sanctions if the policy is not complied with.[106]

While the content and effectiveness of privacy policies are routinely criticised,[107] even this weak protection appears to be breaking down with the advent of eObjects. As implicit human computer interaction techniques become more developed, more eObjects will not need traditional display screens or input mechanisms such as keyboards. Privacy policies require text and screen space, but it is difficult to find a practical way for many eObjects to deliver notice of the data it is collecting, let alone what the vendor or user is planning to do with it. This situation becomes more complicated when the buyer is not the only person about whom data is collected, such as in the case of eObjects with embedded cameras.

---

[104] Eg Autographer, Narrative, SenseCam.

[105] Fanny Coudert, Denis Butin and Daniel Le Métayer, 'Body-worn cameras for police accountability: Opportunities and risks' (2015) 31(6) *Computer Law & Security Review* . See also Steve Mann, 'Wearable Computing' in Mads Soegaard and Rikke Friis Dam (eds), *The Encyclopedia of Human-Computer Interaction* (The Interaction Design Foundation, 2nd ed, 2012) at 23.7 for a discussion of the early history of lifelogging, also known as 'cyborglogging' or 'glogging'.

[106] See for example Gordon Hughes and Lisa di Marco, 'Online privacy policies — it's not just about the Privacy Act' (2015) 18(2) *Internet Law Bulletin* 38 (Australia); Daniel J. Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) *Columbia Law Review* 583 (US).

[107] A long list of articles critical of privacy policies can be found in Roger Clarke, 'The Effectiveness of Privacy Policy Statements' in D Kerr, J Gammack and K Bryant (eds), *Digital Business Security Development: Management Technologies* (IGI Global, 2011) , Part 4.

Early indications are that makers of eObjects are not aware of their own obligations in relation to privacy notices, or are choosing to ignore them (possibly due to weak enforcement mechanisms). A recent survey[108] of 20 popular consumer eObjects ranging from fitness trackers to breathalysers to home automation systems found that none contained a privacy policy packaged with the object, nor any indication where one could be located.[109] Many of the eObjects examined did require an app to be downloaded to make them fully functional, which assumes the use of at least a small screen on a smartphone. However, even in the downloading step, many did not provide a privacy policy or any indication of where to find one.[110]

One example analysed in the survey was that of Breathometer Inc, which currently markets a device that tests alcohol breath levels. The Breathometer device is connected wirelessly to an application on a smartphone, which stores and displays data on current and historical breath levels. There was no privacy policy provided in the package, or as part of the download of the related smartphone application, and there was no information provided in the packaging on where to find one. The author of the survey eventually tracked down a privacy policy in an obscure part of the company's website. This policy prohibits deletion of user data and allows the company to use the data to customise advertisements, as well as other terms.

The lack of connection between the purchase and the privacy terms is troubling:

> Given the many potentially troubling uses for breathalyzer data—think employment decisions; criminal liability implications; and health, life, or car insurance ramifications—one might expect data-related disclosures to dominate the Breathometer user's purchasing and activation experience. Instead, the consumer is essentially led to the incorrect assumption that this small black device is merely a good like any other—akin to a stapler or ballpoint pen—rather than a data source and cloud-based data repository.[111]

The Breathometer purchasing structure is not the most problematic example uncovered by the research. The privacy policy that existed on the Breathometer website was at least specifically designed for the eObject and services sold by the companies. However, many of the other privacy policies examined in the survey, when finally located, had serious issues with their drafting. The wording of the clauses related only to use of the manufacturer's website rather than the eObject itself, and therefore contained considerable ambiguities and key omissions.[112]

Australian Privacy Principle (APP) 1.5 requires that an organisation 'must take such steps as are reasonable in the circumstances to make its … privacy policy available … in such form as appropriate'.[113] Additionally, APP 1.5 includes a Note that 'an APP entity will usually make its APP privacy policy available on the entity's website'. In traditional e-commerce, where goods and services are sold on a website, privacy policies, as well as other terms and

---

[108] Peppet, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent', above n 4.
[109] Ibid, 141 and Appendix 1.
[110] Ibid, 143-146
[111] Ibid, 90.
[112] Ibid, 146.
[113] *Privacy Act 1988* (Cth), Part 1.5, Schedule 1, Australian Privacy Principles.

conditions, at least usually sit within the same virtual 'space' as the purchase (albeit often somewhat obscurely placed). The seller can without any significant uncertainty comply with its obligation in the APP, and a consumer knows where to look. However, meeting the obligation in the APP is not nearly so clear when it comes to eObjects. Suppliers will most likely continue to take the existing cheapest and simplest route of website-based privacy policies. They may or may not change the text of the policies to specifically apply to eObjects, which may then be problematic for both suppliers and consumers. For example, a user's need to know what data is being collected and how it is being used in relation to such eObjects is actually greater than in traditional e-commerce due to:

- eObjects' greater potential to gather data about a purchaser and the people they interact with, such as in the case of a breathalyser, a fitness tracking device or a lifelogging camera; and
- the reduced likelihood of consumers considering the possibility and consequences of data being gathered, stored and used when such activities happen in a less obtrusive way than by active entry of information into a text box.

The meaning of 'appropriate form' is unclear in the context of eObjects, thereby placing it in the context of uncertainty. There is also a potential problem of under-inclusiveness if the Note to APP 1.5 is used as intended as a guide to interpretation by the regulator[114] and judiciary, meaning a supplier could fulfil its obligation merely by placing the policy on its website without other forms of notice to the ultimate user. If eObject purchasing and use activities are completely disconnected from the data-gatherer's website, then it seems insufficient that the only notification is contained there. The unobtrusiveness of the data-gathering function adds to the problems. Consumers using eObjects are viewing themselves as performing physical activities such as breathing out, or walking, or injecting insulin. They are not consciously providing information to a third party as they do when they fill in a website form.

3.7 Autonomy

Autonomous devices and systems are those with the capability to make decisions and take actions that are independent of a human user.[115] Autonomy is a common and desired attribute in eObjects, especially when viewed through the lens of those supporting ambient intelligence scenarios. Where it is present, decisions are made by systems and machines rather than humans. Of course this is often advantageous, as it reduces the need of humans to be involved in low-level decision making when they are only interested in high-level outcomes. For example, a person may regularly be engaged in making presentations in a large organisation with a number of different meeting rooms. A smart office system in conjunction with a mobile device could be programmed to find a person's location within the office, and project the slideshow onto the nearest screen, without any intervention from the user other than a simple instruction to 'run slideshow'.

---

[114] Currently the Office of the Australian Information Commissioner.

[115] Manwaring and Clarke, above n **Error! Bookmark not defined.**, 591, 594, 600-601. For a discussion of the different levels of autonomy that can exist, see Roger Clarke, 'Understanding the drone epidemic' (2014) 30(3) *Computer Law and Security Review* 230.

One current focus for autonomous design in eObjects is the self-driving car. The first tests of a driverless car in the southern hemisphere were undertaken in Adelaide in November 2015,[116] following on from at least 5 years of trials in other countries.[117] Depending on the relevant jurisdiction, 'new' laws may be required to allow driverless cars to be registered and driven on the roads. For example, current New York legislation prohibits drivers from operating a motor vehicle without having at least one hand on the wheel at all times.[118] The rule is clearly directed towards the goal of ensuring that a driver can react quickly to avoid a collision, but is arguably **obsolescent** under Bennett Moses' categorisation in an age where contact with the steering wheel is not required for control.[119]

Not surprisingly, some significant risks have been identified with the capacity of autonomous systems to control decision-making. An autonomous system may well have clear embedded rationales and procedures for its decision-making, but those procedures are usually programmed by someone other than the ultimate user. Moving from current capabilities of autonomous systems to those that might occur in the future, systems that can learn and adapt to environmental change have an even greater capacity to deviate from what is known about the system when it is first installed or interacted with by a user. The risks of this type of autonomous design can include:

- loss of user control; [120]
- unanticipated and undesired behaviours[121] – from the perspective of the primary user and/or others affected by its use[122]; and
- systems which learn to operate outside safe or normal limits, or to conflict with user intentions;[123] and
- the algorithms for decision-making processes and the assumptions behind them may not be accessible to users,[124] which makes them vulnerable to undiscovered error and consequent inappropriate decision-making.

In the case of future developments in driverless cars, the risks of loss of user control and undesired behaviours have recently been the subject of some concern. These concerns concentrate on the possibility of very sophisticated crash-avoidance systems in cars, and the programming of decision-making in the case of an imminent crash that has multiple harmful

---

[116] ABC, *Driverless cars 'could be on roads by 2020', Volvo predicts ahead of first Australian trial* <http://www.abc.net.au/news/2015-11-07/driverless-car-trial-on-southern-expressway/6921060>

[117] Sebastian Thrun, *What we're driving at* <https://googleblog.blogspot.com.au/2010/10/what-were-driving-at.html>

[118] *New York Vehicle & Traffic Law, Title 7*, , s 1226.

[119] The New York legislature has recognised the problems that such a law poses for semi- and fully-autonomous vehicles, and an amending Bill to repeal this section was at the Committee stage as at 30 August 2016. See http://www.nysenate.gov/legislation/bills/2015/s5280 for an up-to-date status.

[120] Poslad, above n 37, 423.

[121] Ibid, 423.

[122] Patrick Lin, 'Here's a Terrible Idea: Robot Cars with Adjustable Ethics Settings' (2014) *Wired (18 August 2014)* <http://www.wired.com/2014/08/heres-a-terrible-idea-robot-cars-with-adjustable-ethics-settings/>.

[123] Poslad, above n 37, 423.

[124] Goodman, above n 62, 6967-89 [Kindle edn].

possible outcomes.[125] Scholars have reformulated the so-called 'trolley problem' thought experiment[126] to apply to self-driving vehicles, for example as:

> You're driving an autonomous car in manual mode—you're inattentive and suddenly are heading towards five people at a farmer's market. Your car senses this incoming collision, and has to decide how to react. If the only option is to jerk to the right, and hit one person instead of remaining on its course towards the five, what should it do?[127]

Other formulations postulate a decision-making algorithm that chooses the safety of the driver over pedestrians, or passengers over drivers.[128] A driver somewhere makes such a decision every day, but usually in a split second, without any real possibility of considering the ethics of his or her decision. The ability of manufacturers to pre-meditate such decisions (or for drivers to choose at leisure particular ethics settings in their cars) may well be seen as a legal problem fitting into Bennett Moses' first category of requiring specially tailored laws required due to the unique nature of new forms of conduct.

4 Conclusion

eObjects with a myriad of different affordances are experiencing significant growth in modern society. With this growth comes change, and with socio-technical change comes the possibility of a disconnection between existing law and the new things, activities, and relationships that arise out of the development and use of eObjects. There exist significant reasons thatlegal researchers and law reform bodies should have the tools and the will to quickly and rigorously analyse and respond to this disconnection. These imperatives include not only the need for timely intervention in circumstances where the Collingridge dilemma is manifested and technologies with detrimental effects may be effectively entrenched by inaction, but also to ensure that any legal reaction is not an overreaction which may inappropriately or prematurely stifle development of beneficial technologies.

This paper has attempted to uncover a diversity of existing and potential legal problems that might arise in different contexts arising out of the development of the third wave of computing. This analysis has not only identified specific legal problems in particular areas but also some problems more general in their application, which are worth further investigation. Firstly, but not surprisingly, uncertainty has emerged as a significant issue, with important consequences. Rule-making bodies must find ways to deal appropriately with the Collingridge dilemma. Otherwise, regulation runs the risk of stifling beneficial innovative practices or being inadequate to protect users' legitimate interests. The likelihood of the latter is heightened by the fact that the most likely reaction of manufacturers and suppliers to risks posed by uncertainty will be an attempt to exclude liability through contractual terms and conditions. These (usually) non-negotiable terms and conditions, including clauses relating to privacy and data protection, pose particular

---

[125] Similar questions have been raised in work relating to robotics eg Roger Clarke, 'Asimov's laws of robotics: implications for information technology - Part I' (1993) 26(12) *Computer* 53 and Roger Clarke, 'Asimov's laws of robotics: Implications for information technology - Part II' (1994) 27(1) *Computer* 57.

[126] Eg as described in Judith J. Thomson, 'Killing, Letting Die, and the Trolley Problem' (1976) 59(2) *The Monist* 204.

[127] Patrick Lin quoted in Lauren Cassani Davis, 'Would You Pull the Trolley Switch? Does it Matter?' (2015) *The Atlantic (9 October 2015)* <http://www.theatlantic.com/technology/archive/2015/10/trolley-problem-history-psychology-morality-driverless-cars/409732/>.

[128] Lin, above n 122.

risks for individual users.[129] The limitations on text display of many consumer eObjects means that forms of consent are often questionable, and proper notice of terms contested. Secondly, the category of under-inclusiveness has emerged as critical when considering new conduct made possible by eObjects. Under-inclusiveness (as well as over-inclusiveness) will often give rise to a competition of interests. Therefore, when faced with questions of under- or over-inclusiveness of new products, activities and relationships arising out of new technologies, rule-making bodies will need to make significant policy decisions as to whose interests should be given priority. For should those detrimentally affected by the conduct be protected at the expense of those making a commercial return from the conduct, or should commercial interests prevail?

Due to the diversity of both the technologies concerned, and the areas of law and regulation that may be affected, this paper cannot provide a comprehensive analysis of all legal problems that might arise out of the new activities, things and relationships made possible by eObjects. The emphasis in this paper has been on demonstrating the utility of a particular approach relevant to eObjects, and an indication of the diversity of the issues that might arise. The approach is not limited to any one area of the law, nor to the specific eObjects discussed in detail. This paper is intended to provide a roadmap for further research into any and all legal problems arising out of the new activities, products and relationships made possible by eObjects. For example, further research may analyse legal problems that arise out of a particular subset of eObjects, for example driverless cars, or those that arise in a particular industry, such as healthcare.

[129] See eg Margaret Jane Radin, *Boilerplate : the fine print, vanishing rights, and the rule of law* (Princeton, N.J. : Princeton University Press 2013).

Appendix – core and common attributes of eObjects[130]

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

Human computer interaction (HCI) - can be unobtrusive or invisible, or contain different levels of implicit HCI

Identifiability - has an identifier for the physical object

Network Locatability - locatable in virtual space

Mobility

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

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

---

[130] Manwaring and Clarke, above n **Error! Bookmark not defined.**, Tables 2 and 3, 599-601.

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

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

Bibliography

Articles/Books/Reports

Adelstein, Frank et al, *Fundamentals of mobile and pervasive computing* (McGraw-Hill, 2005)

Albatal, Rami et al (eds), *Shaping our digital lives* (2014)

Barcena, Mario Ballano, Candid Wueest and Hon Lau, Symantec Security Response Report, 11 August 2014, *How safe is your quantified self?*

Bennett Moses, Lyria, 'Recurring dilemmas: the law's race to keep up with technological change' (2007) 2 *University of Illinois Journal of Law, Technology & Policy* 239

Bennett Moses, Lyria, 'Why have a theory of law and technological change?' (2007) 8(2) *Minnesota Journal of Law, Science & Technology* 589

Bennett Moses, Lyria, 'Agents of Change: How the Law Copes with Technological Change' (2011) 20 *Griffith Law Review* 763

Bennett Moses, Lyria, 'How to Think about Law, Regulation and Technology – Problems with "Technology" as a Regulatory Target' (2013) 5(1) *Law, Innovation and Technology* 1

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

Brownsword, Roger, *Rights, Regulation, and the Technological Revolution* (Oxford University Press, 2008)

Brownsword, Roger and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge University Press, 2012)

Bruce, Alex, *Consumer Protection Law in Australia* (LexisNexis Butterworths, 2nd ed, 2014)

Calo, Ryan, 'Digital Market Manipulation' (2014) 82(4) *George Washington Law Review* 995

Cassani Davis, Lauren, 'Would You Pull the Trolley Switch? Does it Matter?' (2015) *The Atlantic (9 October 2015)* <http://www.theatlantic.com/technology/archive/2015/10/trolley-problem-history-psychology-morality-driverless-cars/409732/>

Checkoway, Stephen et al, 'Comprehensive Experimental Analyses of Automotive Attack Surfaces' in D Wagner (ed), *Proceedings of USENIX Security 2011, Aug 2011* (USENIX, 2011)

Cimpanu, Catalin, 'Insecure Internet-Connected Kettles Help Researchers Crack WiFi Networks Across London' (2015) *Softpedia (20 October 2015)* <http://news.softpedia.com/news/insecure-internet-connected-kettles-help-researchers-crack-wifi-networks-across-london-494895.shtml>

Clarke, Roger, 'A Framework for Analysing Technology's Negative and Positive Impacts on Freedom and Privacy (Draft of 16 August 2015)' <http://www.rogerclarke.com/DV/Biel15-DuDA.html#App3>

Clarke, Roger, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms (last updated 21 October 2013)' <http://www.rogerclarke.com/DV/Intro.html#Mis>

Clarke, Roger, 'Asimov's laws of robotics: implications for information technology - Part I' (1993) 26(12) *Computer* 53

Clarke, Roger, 'Asimov's laws of robotics: Implications for information technology - Part II' (1994) 27(1) *Computer* 57

Clarke, Roger, 'Paradise gained, paradise re-lost: how the Internet is being changed from a means of liberation to a tool of authoritarianism' (2001) 18(August 2001) *Mots Pluriels*

Clarke, Roger, 'The Effectiveness of Privacy Policy Statements' in D Kerr, J Gammack and K Bryant (eds), *Digital Business Security Development: Management Technologies* (IGI Global, 2011)

Clarke, Roger, 'Understanding the drone epidemic' (2014) 30(3) *Computer Law and Security Review* 230

Clarke, Roger and Alana Maurushat, 'Passing the Buck: Who Will Bear the Financial Transaction Losses from Consumer Device Insecurity?' (2007) 18 *Journal of Law, Information & Science* 8

Cloud Security Alliance Mobile Working Group, *Security Guidance for Early Adopters of the Internet of Things (IoT) (April 2015)* (2015)

Cockfield, Arthur J., 'Towards a law and technology theory' (2004) 30(3) *Manitoba Law Journal* 383

Collingridge, David, *The social control of technology* (Pinter, 1980)

Coudert, Fanny, Denis Butin and Daniel Le Métayer, 'Body-worn cameras for police accountability: Opportunities and risks' (2015) 31(6) *Computer Law & Security Review*

Coulouris, George F et al, *Distributed systems : concepts and design* (Addison-Wesley (Pearson Education), 2012)

Davison, Robert M., 'The privacy rights of cyborgs' (2012) 27 *Journal of Information Technology* 324

Dionne, Daniel, 'Explainer: what is geoblocking?' (2013) *The Conversation* <https://theconversation.com/explainer-what-is-geoblocking-13057>

Dourish, Paul and Genevieve Bell, *Divining a digital future: mess and mythology in ubiquitous computing* (MIT Press, 2011)

Evans, David, '*The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper, April 2011' (2011)

Finn, Rachel L, David Wright and Michael Friedewald, 'Seven Types of Privacy' in Serge Gutwirth et al (eds), *European Data Protection: Coming of Age* (Springer, 2013) 3-32

Fogg, B. J., *Persuasive technology : using computers to change what we think and do* (Amsterdam ; Boston : Morgan Kaufmann Publishers, 2003)

Gellert, R. and S. Gutwirth, 'The legal construction of privacy and data protection' (2013) 29(5) *Computer Law & Security Review* 522

Giblin, Rebecca, 'Stranded in the Technological Dark Ages: Implications of the Full Federal Court's decision in NRL v Optus' (2012) 35 *European Intellectual Property Review* 632

Gibson, William, 'Burning Chrome (short story)', *Burning Chrome* (Harper Collins, 1995)

Godara, Varuna (ed), *Risk assessment and management in pervasive computing operational, legal, ethical, and financial perspectives* (Information Science Reference, 2009)

Goodman, Marc, *Future crimes : everything is connected, everyone is vulnerable and what we can do about it* (Doubleday, 2015)

Greenberg, Andy, '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/>

Greenberg, Andy 'GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars', *Wired*, 10 Sep 2015 <http://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/>

Helberger, Natali, '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, Geof and Frank Zeichner, ''Enabling the Internet of Things for Australia: Measure, Analyse, Connect, Act' (Industry Report, Communications Alliance Ltd, October 2015)'

Hildebrandt, Mireille, 'A Vision of Ambient Law' in Roger Brownsword and Karen Yeung (eds), *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes* (Hart Publishing, 2008)

Hildebrandt, Mireille, *Smart technologies and the end(s) of law : novel entanglements of law and technology* (Edward Elgar Publishing, 2015)

Hildebrandt, Mireille and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) *Modern Law Review* 428

Hill, Kashmir, 'Crib Cams: Watch out new parents - internet-connected baby monitors are easy to hack' (2015) *Fusion.net (3 Sep 2015)* <http://fusion.net/story/192189/internet-connected-baby-monitors-trivial-to-hack/>

Hughes, Gordon and Lisa di Marco, 'Online privacy policies — it's not just about the Privacy Act' (2015) 18(2) *Internet Law Bulletin* 38

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

King, Kevin, 'Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 *Albany Law Journal of Science & Technology* 61

King, Nancy J, 'When Mobile Phones Are RFID-Equipped — Finding EU-US Solutions to Protect Consumer Privacy and Facilitate Mobile Commerce' (2008) 15 *Michigan Telecommunications & Technology Law Review* 107

Kirby, Michael, 'The Fundamental Problem of Regulating Technology' (2009) 5 *The Indian Journal of Law and Technology* 1

Koops, Bert-Jaap, 'Ten dimensions of technology regulation. Finding your bearings in the research space of an emerging discipline' in Morag Goodwin, Bert-Jaap Koops and Ronald Leenes (eds), *Dimensions of Technology Regulation* (Wolf Legal Publishing, 2010) 309-324

Kurosu, Masaaki (ed), *Towards Intelligent and Implicit Interaction* (Springer, 2013)

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

Li, Grace, 'Deciphering Pervasive Computing: a Study of Jurisdiction, E-Fraud and Privacy in Pervasive Computing Environment' in Varuna Godara (ed), *Risk Assessment and Management in Pervasive Computing: Operational, Legal Ethical and Financial Perspectives* (Information Science Reference, 2009) 218-245

Lin, Patrick, 'Here's a Terrible Idea: Robot Cars with Adjustable Ethics Settings' (2014) *Wired (18 August 2014)* <http://www.wired.com/2014/08/heres-a-terrible-idea-robot-cars-with-adjustable-ethics-settings/>

Macdonald, Barbara, 'Legislative Intervention in the Law of Negligence: The Common Law, Statutory Interpretation and Tort Reform in Australia ' (2005) 27(3) *Sydney Law Review* 443

Mann, Steve, 'Wearable Computing' in Mads Soegaard and Rikke Friis Dam (eds), *The Encyclopedia of Human-Computer Interaction* (The Interaction Design Foundation, 2nd ed, 2012)

Manwaring, Kayleen, 'Enforceability of Clickwrap and Browsewrap Terms in Australia: Lessons from the U.S. and the U.K' (2011) 5(1) *Studies in Ethics, Law, and Technology* Article 4

Manwaring, Kayleen, 'A shift in time saves no-one: mobile technologies and the NRL v Optus decision' [83] (2012) 5(No 1 & 2) *Journal of the Australasian Law Teachers Association* 83

Manwaring, Kayleen and Roger Clarke, 'Surfing the third wave of computing: a framework for research into networked eObjects' (2015) 31(5) *Computer Law & Security Review* 586

Mao, Y. et al, 'Sponge-Like Piezoelectric Polymer Films for Scalable and Integratable Nanogenerators and Self-Powered Electronic Systems' (2014) 4(7) *Advanced Energy Materials*

Marchant, Gary E, Braden R Allenby and Joseph R Herkert (eds), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (Springer, 2011)

Michael, Katina and Roger Clarke, 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' (2013) 29 *Computer Law & Security Review* 216

Noto La Diega, Guido and Ian Walden, 'Contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016' (2016) <http://ssrn.com/abstract=2725913>

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

Peppet, Scott R, 'Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security & Consent' (2014) 93(1) *Texas Law Review* 85

Poslad, Stefan, *Ubiquitous computing: smart devices, environment and interaction* (John Wiley & Sons Ltd, 2009)

Radin, Margaret Jane, *Boilerplate : the fine print, vanishing rights, and the rule of law* (Princeton, N.J. : Princeton University Press, 2013)

Rahman, Mahmudur, Bogdan Carbunar and Madhusudan Banik, 'Fit and Vulnerable: Attacks and Defenses for a Health Monitoring Device' (2013) *arXiv:1304.5672 [cs.CR]*

Reddy, Trips, '15 Companies From Airports to Retail Already Using Beacon Technology' (2014) <https://www.umbel.com/blog/mobile/15-companies-using-beacon-technology/>

Robertson, Jordan, 'Insulin pumps, monitors vulnerable to hacking' (Pt Fairfax) (2011) *Sydney Morning Herald* <http://news.smh.com.au/breaking-news-technology/insulin-pumps-monitors-vulnerable-to-hacking-20110804-1idfn.html>

Satyanarayanan, Mahadev, 'Fundamental challenges in mobile computing' (Pt ACM) (1996) *Principles of distributed computing: Proceedings of the fifteenth annual ACM symposium* 1

Satyanarayanan, Mahadev, 'Pervasive computing: vision and challenges' (2001) 8(4) *IEEE Personal Communications* 10

Schneier, Bruce, 'The Internet of Things is Wildly Insecure - and often Unpatchable' (2014) *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/>

Smith, Matt, 'Why your smartphone won't be your next PC' (2013) *3 August 2013 Digital Trends* <http://www.digitaltrends.com/computing/why-your-smartphone-wont-be-your-next-pc/#!US6P1>

Solove, Daniel J. and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114(3) *Columbia Law Review* 583

Thierer, Adam D. , 'The Internet of Things & Wearable Technology: Addressing Privacy & Security Concerns Without Derailing Innovation' (2015) 21(2) *Richmond Journal of Law & Technology*

Thomson, Judith J., 'Killing, Letting Die, and the Trolley Problem' (1976) 59(2) *The Monist* 204

Townsend, Anthony M., *Smart cities: big data, civic hackers, and the quest for a new utopia* (W. W. Norton & Company, 2013)

Uteck, Anne, *Reconceptualizing Spatial Privacy for the Internet of Everything* (PhD thesis Thesis, University of Ottawa, 2013)

Vulkanovski, Alexander, "*"Home, Tweet Home"*: Implications of the Connected Home, Human and Habitat on Australian Consumers', report for Australian Communications Consumer Action Network (ACCAN), Feb 2016' (2016)

Walker Smith, Bryant 'Proximity-Driven Liability' [1777] (2013-2014) 102 (6) *Georgetown Law Journal* 1777

Weber, Rolf H., 'Internet of things – New security and privacy challenges' [23] (2009) 26(1) *Computer Law and Security Review: The International Journal of Technology and Practice* 23

Weiser, Mark, 'The Computer in the 21st Century' (Pt 1991) [94] (1991) *Scientific American* 94

Werbach, Kevin, 'Sensors and Sensibilities' [2321] (2007) 28(5) *Cardozo L. Rev.* 2321

Wood, James, 'iBeacon: the Future of Content Marketing?' (2014)(7 October 2015) *B2B Marketing* <http://www.b2bmarketing.net/blog/posts/2014/02/17/ibeacon-future-content-marketing>

Wright, David et al (eds), *Safeguards in a world of ambient intelligence* (Springer, 2008) vol 1

Zetter, Kim, 'Medical devices that are vulnerable to life-threatening hacks' (2015) *Wired.com* <http://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/#slide-x>

Cases

eBay International AG v Creative Festival Entertainment Pty Limited (2006) eBay International AG v Creative Festival Entertainment Pty Limited [2006] FCA 1768

Federal Trade Commission v Wyndham Worldwide Corporation [2015] Federal Trade Commission v Wyndham Worldwide Corp, No 14-3514, F 3d (Aug 24, 2015))

Miller & Associates Insurance Broking Pty Ltd v BMW Australia Finance Ltd [2010] HCA 31

National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd [2012] FCAFC 59

Legislation

15 US Code § 45 - Unfair methods of competition unlawful; prevention by Commission

18 US Code § 1030 - Fraud and related activity in connection with computers,

Competition and Consumer Act 2010 (Cth)

Computer Misuse Act 1990 (UK)

Crimes Act 1900 (NSW)

Crimes Act 1958 (Vic)

Criminal Code 1899 (Qld)

Criminal Code 2002 (ACT)

Criminal Code Act 1924 (Tas)

Criminal Code Act 1995 (Cth)

Criminal Code Compilation Act 1913 (WA)

Family Law Act 1975 (Cth)

Fatal Accidents Act (1846) 9 & 10 Vict c 93 (NSW)

New York Vehicle & Traffic Law, Title 7,

Privacy Act 1988 (Cth)

SPY Car Act of 2015, S 1806, 114th Congress (2015)

Summary Offences Act 1953 (SA)

Other

ABC, *Driverless cars 'could be on roads by 2020', Volvo predicts ahead of first Australian trial* <http://www.abc.net.au/news/2015-11-07/driverless-car-trial-on-southern-expressway/6921060>

Federal Trade Commission, 'ASUS Settles FTC Charges That Insecure Home Routers and “Cloud” Services Put Consumers’ Privacy At Risk') <https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put>

Gartner, 'Gartner Says 4.9 Billion Connected "Things" Will Be in Use in 2015' (2014) <http://www.gartner.com/newsroom/id/2905717>

Open Web Application Security Project, *Top 10 IoT Vulnerabilities (2014) Project* Open Web Application Security Project Wiki <https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=Top_10_IoT_Vulnerabilities__282014_29>

Thrun, Sebastian, *What we’re driving at* <https://googleblog.blogspot.com.au/2010/10/what-were-driving-at.html>

Weiser, Mark and John Seely Brown, *The Coming Age of Calm Technology* (5 October 1996) <http://www.ubiq.com/hypertext/weiser/acmfuture2endnote.htm>