SOCIAL LICENCE AND THE INTERNET OF THINGS

A REPORT PREPARED FOR THE DATA FUTURES PARTNERSHIP

JULY 2016

REPORT PREPARED BY MARTIN PERRY

INDEPENDENT RESEARCH CONTRACTOR

WELLINGTON

ABOUT THIS DOCUMENT

The Internet of Things is enabling large numbers of previously unconnected devices to communicate data and to be controlled remotely, either directly by other connected devices or with human intervention. The benefits of increased connectivity are expected to transform many sectors of activity including agriculture, healthcare, energy, transport and the management of infrastructure. For individuals, the Internet of Things promises to transform everyday life through innovations associated with such things as wearable computing, the 'quantified self' and home technology or 'domotics'.

This report is about the 'social licence' issues that may impede the ability to capture the benefits of the Internet of Things or that may slowdown public acceptance of increased connectivity, rather than being about the benefits that will be created. As a contribution to the work of the Data Futures Partnership, the report is primarily about what may affect the public's acceptance of the forms and level of data collection implied by the rapidly emerging Internet of Things. The scope of the report is limited to a review of the issues that have been identified through an examination of media articles, government agency reports, academic writing and campaign group websites.

The report has benefited from comments received by members of the Data Futures Partnership, but report's author is solely responsible for the content of the report.

About the Data Futures Partnership

The Partnership is an independent group that was created by Government to develop innovative solutions to data-use issues. The Partnership's work is directed by a Working Group that was appointed by Cabinet. The Working Group is supported by a secretariat housed at Statistics NZ.

The Partnership has been created to make a positive impact across the data-use ecosystem, by bringing together a cross-sector group of influential individuals who can work together and provide a collective voice on data issues.

It has been mandated by Government to engage with citizens, the private sector, and non-government organisations to help drive change across New Zealand's data-use ecosystem.

See: http://datafutures.co.nz

SOCIAL LICENCE AND THE INTERNET OF THINGS

SUMMARY

This review identifies the 'social licence' issues that have been associated with the use and exchange of data collected by the Internet of Things (IoT). The IoT is based on machine-to-machine communication and enables more of the physical and natural world to be integrated into and to become accessible via the Internet.

Government agencies are expressing concern about the lack of public awareness over the IoT and the problems that this may pose. People working in the area of new technology expect the IoT to become a reality, while expressing doubts over some aspects of the change that may come about. Technology standardisation, interoperability and infrastructure capacity are among concerns over the feasibility of widespread diffusion.

One assessment identifies four unanswered questions about the IoT: How will the 'things' talk to each other? Who can see the data? How secure is the Internet of Things? If a system malfunctions, who is to blame?

Privacy is expected to be harder to protect as the IoT becomes established. The ability to manage privacy through 'notice and consent' is questioned. A use-focused privacy regime has been proposed as more suited to the IoT than current privacy protection principles.

A major data breach or cyber-attack is likely to have damaging consequences for public acceptance of the IoT. Several inherent features of the IoT have been identified that make data security hard to manage.

The use of algorithms to turn IoT data into information attracts comment because of the lack of data transparency and risk that this may hide discrimination.

While the IoT is global in scope, it is presently governed by national laws. A need for some form of global governance is advocated by some legal experts.

Consumer protection and empowerment is necessary aspect of building trust in the IoT (along with privacy and security). Consumer protection is based upon adequate information disclosure, fair commercial practices including quality of service, and dispute resolution and redress. There is currently too little understanding among consumers and a need for more certainty over the ability of consumers to make informed decisions about their use of IoT devices.

Four applications of the IoT commented upon in the review are Ageing in place, Connected vehicles, Retail environments, Smart homes.

SOCIAL LICENCE AND THE INTERNET OF THINGS

This review identifies the 'social licence' issues that have been associated with the use and exchange of data collected by the Internet of Things (IoT). It addresses the opportunities, questions, concerns and ethical considerations that have been identified as influencing people's interest, involvement and acceptance of services and activities facilitated by the IoT.

The existing Internet differs from the IoT mainly according to the range of devices that are enabled to communicate and share data through the Internet. Some form of computing device is needed to transmit data via the Internet. The IoT enables more of the physical and natural world to be integrated into and to become accessible via the Internet, including both animate and inanimate objects. One definition of the IoT is:

> The network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment (Gartner IT Glossary).

A recent OECD (2015) review of the digital economy supports a broader definition of the IoT that covers all devices and objects whose state can be altered by the Internet (OECD 2015: 244). This broader conception is to explicitly include person-operated/controlled devices such as smart phones, laptops and tablets as part of the IoT.

Machine-to-machine connectivity first gave rise to the concept of the IoT, and some still view it as the most transformational aspect of the IoT (Caron et al. 2016: 5). The OECD's definition captures how many newly connected objects will continue to be controlled by people. This underlines how the IoT will be affected by what people perceive to be its relative costs and benefits.

Scope of the review

The literature on which this review is based is sourced mainly from two literature databases covering academic and media publications: the Web of Science and Business Source Complete. Media reports and government agency reports were identified through the Financial Times database with other literature obtained through the Massey University library collection database.

The review was directed to give particular attention to cases where public reaction is affecting the acceptance of the IoT. As a technology that is still developing and whose operation is not always evident, the review is based mainly on comment and evaluation from public agencies, academics and campaign groups. Public agencies in North America and Europe are examining what regulatory responses may be required to balance the economic benefits of the IoT with the increased risks to privacy and security. Reports and submissions of privacy campaign groups (Table 1) are drawn upon, recognising that these groups are actively seeking to influence the

debate about the public acceptability of data collection practices associated with the IoT.

Table 1 Privacy campaign groups active in raising concerns about the IoT

Future of Privacy Forum – https://fpf.org	A Washington-based think tank that seeks to advance responsible data practices.
Privacy International – https://www.privacyinternational.org	A UK-based NGO 'fighting for the right to privacy across the world. We investigate the secret world of government surveillance and expose the companies enabling it'.
Electronic Privacy Information Centre – https://www.epic.org	A Washington-based research centre established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age.

Rather than public debate about the IoT driving public agency interest, government agencies are expressing concern about the lack of public awareness and the problems that this may pose. For example, in evidence to a government enquiry in the UK, the Competition & Markets Authority comments:

> …pressure on consumers is only set to increase. Developments such as the Internet of Things—like online devices we wear or carry and devices in the home or in our cars—will mean that data is collected and shared on a regular basis without the consumer having to make a conscious decision. (House of Lords Select Committee on European Union 2016: 59).

The enquiry report goes on to say:

> …the complex ways in which online platforms collect and use personal data mean that the full extent of this agreement is not sufficiently understood by consumers. As a result, trust in how online platforms collect and use consumers' data is worryingly low and there is little incentive for online platforms to compete on privacy standards. We believe this presents a barrier to future growth of the digital economy. (House of Lords Select Committee on European Union 2016: 59).

In a similar vein, the OECD (2015: 271) say that a lack of awareness about the IoT promotes uneasiness about and resistance to its development.

Report structure

The basic structure of the report is shown in Figure 1.

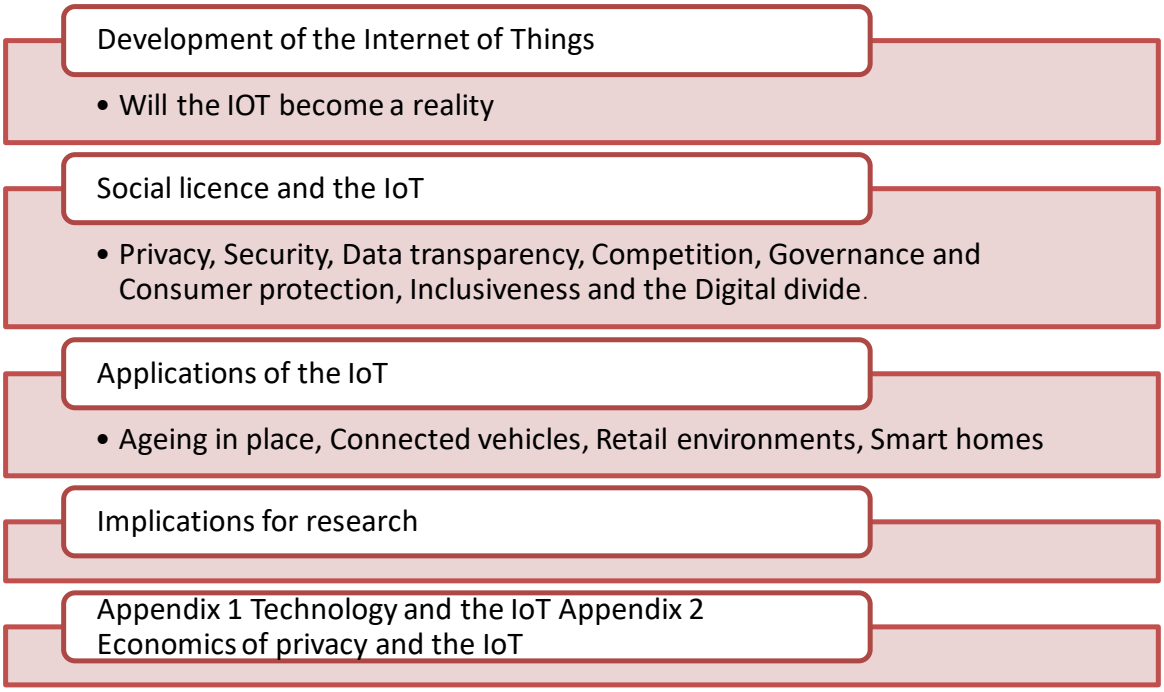

Figure 1: Structure of the report

Development of the Internet of Things

The Internet of Things (IoT) describes a world in which everyday objects are connected to a network so that data can be shared (UK Government Chief Scientific Advisor 2014). A 'thing' in the context of the IoT can be anything large enough to contain a wireless transmitter (employing Wi-Fi, Bluetooth or any other wireless protocol) and unique enough to be assigned its own Internet Protocol (IP) address (Miller 2015: 8).

Embedding objects with limited processor, memory, communication and power resources opens up an array of potential applications. For example, data can be collected in buildings, factories, public spaces and natural environments with application in urban planning, manufacturing and environmental monitoring (OECD 2015: 240). The value of connectivity will vary according to whether the IoT connects 'physical first' or 'digital first' objects (Greengard 2015:16).

- Physical first objects do not typically generate or communicate digital data unless augmented or manipulated.
- Digital first objects are capable of generating data and communicating it on for further use, inherently and by design.

By collecting and transmitting more data, digital first objects offer greater opportunity for generating original insights than do physical first objects. A tagged hardbound book, for example, may reveal its location. A tagged e-book can reveal to a marketer how the reader uses and reads the book, as well as where the book is read.

Appendix 1 provides some further information on data collection technology associated with the IoT. By enabling more of the physical and natural world to become connected, greater connectivity is expected to bring something more than simply an enhanced Internet (Weinberg et al. 2015:617) (Table 2).

Table 2 Key distinctions between the Internet and the Internet of Things in terms of how consumer-related data is captured and used

Data collection and utilisation	Internet	Internet of Things
Data	Mainly online/digital in origin, collected in an environment/context largely constructed by providers of data	Data sourced in the real world, environment/context largely 'natural', with many aspects/contexts potentially yielding data
Data entry	Data harvested from active, deliberate actions (eg. mouse clicks, web browsing)	Data obtained without consumer action, using devices not controlled by the consumer
Data sharing	With other data collectors, providers & analysts	With other devices, as well as with other data collectors, providers & analysts
Learning from data	Consumer behaviour learnt from web-related behaviour	Consumer behaviour learnt from real world behaviour as well as the web-related activity
Data application in decision making	Frequently a time lag between data collection, processing and decision making responses	Constant monitoring and real time machine-mediated responses and decision making

Source: Based on Weinberg et al. 2015:617-619)

In a Web-based environment, for example, consumer behaviour is captured through website cookies and similar monitoring software. In an IoT-based environment, consumer behaviour can be studied in the 'natural', non-digital world with no need for the consumer to be engaged with the online environment. For example, IoT devices could examine how the temperature within a building affects consumer behaviour and use temperature settings to influence consumer behaviour (Weinberg et al. 2015:617).

Will the IoT become a reality?

In the USA, the Pew Research Centre Internet Project obtained the views of nearly 1,600 IT experts to inform an assessment of the future of the IoT (Anderson and Rainie 2014). Of these informants, 83 percent agreed that the IoT will have widespread and beneficial effects on the everyday lives of the public by 2025. Coming from people developing and benefiting from new technology, the responses may overestimate the IoT's impact (Greengard 2015: 188). But if the respondents are

'technology optimists', they also have doubts over some aspects of the change that may come about (Table 3).

Table 3 Themes in the Pew Research Centre study of the IoT in 2025

Themes in the 2014 Pew Research Centre report on the future of the IoT
The realities of this data-drenched world raise substantial concerns about privacy and people's abilities to control their own lives. If many everyday activities are monitored and people are generating informational outputs, the level of profiling and targeting will grow and amplify social, economic, and political struggles.
Information interfaces will advance—especially voice and touch commands. But few expect that brain-to-network connectivity will be typical in most daily lives in 2025.
There will be complicated, unintended consequences: 'We will live in a world where many things won't work and nobody will know how to fix them.'
The unconnected and those who just don't want to be connected may be disenfranchised. Consider the ramifications of digital divides.
Individuals' and organisations' responses to the Internet of Things will recast the relationships people have with each other and with groups of all kinds.

Source: Anderson and Rainie (2014)

Of more immediate practical importance, level, the availability of wireless spectrum will shape the development of the IoT (Ofcom 2015). In the UK, this is expected to see the initial uptake of the IoT concentrated on smart metering networks, applications utilising purposively developed IoT networks (which in the UK are being rolled out in 10 smart city projects) and applications that can be supported by existing and future mobile networks (Ofcom 2015: 10). The OECD (2015: 253) discusses ways of overcoming the need for wireless spectrum, such as utilising unused frequencies in the television bands.

Nonetheless, while some impact is already being felt, uncertainty exists as to how far and how quickly the IoT will become a reality. The Office of the Privacy Commissioner of Canada (2016) groups the challenges into three main types.

- The cost of sensors and actuators need to fall to levels that will spark widespread use. (Separately, for example, Palmer (2015) reports that the price for the technology to connecting things needs to fall to around $6 from the present $40-$80.)
- Interoperability and security standards need to be established for sensors, computers and actuators. (Separately, in relation to standards, the UK Government Chief Scientific Advisor (2014: 16) notes that there are not yet any clear 'winners' for interpreting the data from devices or for connecting them to one another.)

- Privacy and security concerns must be addressed in a meaningful way.

To reach its full potential, a UK Parliamentary Library (2015) briefing note identifies four main questions to be answered about the implementation of the IoT (Table 4).

Table 4 Four unanswered question about the IoT

How will the 'things' talk to each other?	In most cases this will be via wireless network. The various technologies available, such as Wi-Fi, Bluetooth, 3G and 4G, use different communications protocols and common standards are needed to integrate the IoT with these technologies. Competition for spectrum with navigation, broadcasting and communications services is a potential issue in the long term.
Who can see the data?	The devices making up the Internet of Things will harvest vast quantities of data. Consumer controls over the data they share exist, but there are still concerns that the data could be used in ways that infringe privacy.
How secure is the Internet of Things?	Traditional approaches to security (such as running software upgrades) may not be practical to implement given the number of IoT devices. There have already been examples of hackers gaining access to data from webcams, baby monitors, CCTV cameras and even fridges. Using specialist equipment and expertise, security researchers have even shown that it is possible to breach some medical devices and cars. Robust and secure communications networks are needed.
If a system malfunctions, who is to blame?	Is it the user, the manufacturer, or the person who installs the system? This is just one example of an area where the Internet of Things is likely to create new regulatory challenges.

Source: UK Parliamentary Library (2015)

The interoperability of devices has been identified by the OECD (2015: 271) has important for consumer trust in the IoT. As well as the standardisation of technologies to allow products to be integrated, software update management challenges will need to be overcome to maintain interoperability between older and newer devices.

Social licence and the Internet of Things

The impact for individual autonomy is perhaps the most fundamental source of concern that may slow down the acceptance of the IoT (Weinberg et al. 2015: 621).

This is the perception that as more data are used to define and influence people, individuals will be faced with less discretion over their everyday affairs. A person's ability to separate their personal and professional (work) life also risks further erosion. As more aspects of a person's life become connected via the Internet, so employers (existing and prospective) have more capacity to search and learn about an employee's, a prospective employee's, or a consumer's personal life.

Large questions also exist over whether 'smart systems' mean 'dumb people' through the tendency to gravitate to the simplest and most pleasing way of doing things (Greengard 2015: 147). Risks of an over-dependence on technology, obtains comment too. As automated systems become more reliable and efficient, human dependence on complex technology grows. Better technology can reduce the chances of automation failing, but the severity of a failure can become ever more severe.

Viewing the IoT less as a monolithic technology, and more as a multiplicity of applications is one response to such fundamental questions. Such a view is expressed by the UK Government Office for Science (2014: 10) who notes:

> Like any new technology it [the IoT] should not be considered generically as 'good' or 'bad'. Each use needs to be considered specifically.

In order to ensure that the IoT works for the benefit of people, the OECD (2015: 266) argues that it needs to be an 'Internet of Trust'. Trust is fundamental to enhancing user experience as without trust, participation will fall. Trust will also affect the perceived adequacy of legal controls and need for additional regulatory action. The OECD identifies security, privacy and consumer protection as three areas critical to building an Internet of Trust.

The UK Government Chief Scientific Adviser (2014) draws on evidence from studies of public reactions to similar emerging technologies to identify four themes shaping the public's reaction to the IoT.

- Concerns about privacy, safety and security and related demands for accountability and (anticipatory) governance.
- Desire for competition, choice (including opt-out choices) and questions of unintended consequences and liability.
- Clarity on who is in control and who is driving the development and direction of research.
- Consideration for the winners and losers from the introduction of technologies and concern if the changes are perceived to exacerbate inequality.

Based on these assessments, the following sections examine the issues raised in the areas of privacy, data transparency, security, competition, governance and consumer protection, inclusiveness and the digital divide.

Privacy and the IOT

Privacy principles require that users should be able to keep control of their data and be able to opt out of sharing personal data without incurring negative consequences (Office of the Privacy Commissioner of Canada 2016: 16). Privacy is expected to be harder to protect as the IoT becomes established. Two recent cases in the USA illustrate companies exploiting the increased capacity to collect information about individuals: 'Brightest flashlight' and InMobi.

Brightest Flashlight app

The Android app Brightest Flashlight has been installed by millions of smart phone users, with many (perhaps most) unaware that the app collected and shared location and device ID information.

The app's privacy policy had mentioned that information collected would be used by the company, but the information was shared automatically with advertisers and other third parties, before consent was obtained and even when users opted out.

In 2014, the Federal Trade Commission in the USA settled a complaint that the supplier of the app had deceived consumers with a privacy policy that did not reflect the app's use of personal data and presented consumers with a false choice on whether to share their information.

The settlement also requires the defendants to provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared. An affirmative express consent is now required before the data can be collected.

https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app

InMobi's location tracking software

InMobi's software is designed to enable app developers to make money from advertisers. The software can tell an advertiser an app user's precise location and location movements over the previous two months.

Prior to December 2015, even when an app user had selected 'no' to disable the app's location tracking request (or turning it off manually), InMobi used information collected from Wi-Fi networks to enable app developers to pass on location information.

The US Federal Trade Commission reached a settlement with InMobi in June 2016 to require InMobi to obtain consent for any form of location tracking.

https://fpf.org/2016/06/22/ftc-settles-major-ad-platform-deceptive-location-tracking-via-wi-fi/

The Brightest Flashlight and InMobi cases involve deceptive practices, dealt with by existing consumer protection regulation. Nonetheless, they fit with concerns that have been expressed about the extent to which the IoT presents new challenges to traditional principles of privacy control.

The OECD (2015: 266) argues that the enormous increase in and complexity of data gathering with the IoT makes it more difficult for individuals to control and police data collection. The basic problem is that, as in the Brightest Flashlight and InMobi cases, individuals are frequently unaware that the data are being collected. Based on a review of academic literature, Caron et al. (2016: 8) identify four areas of privacy concern (Table 5).

Table 5 Areas of privacy concern identified in academic literature

Aspect of privacy	Ethical issue	Explanation
Unauthorised surveillance	Privacy – what information to keep/reveal	Data collection on a large scale implies widespread tracking risks (monitoring of actions, movement and communications) of people without their knowledge or consent.
Uncontrolled data generation and use	Accuracy – authenticity, accuracy and responsibility	Control over the generation and use of the collected data, its owner and its diffusion (disclosure of information: exchange and transfer).
Inadequate authentication	Property – who owns the information	Access control deals with ensuring the identity of a service, of its customer (regarding its anonymity right) and the user's access grants authorisation.
Information security risks	Accessibility – rights to obtain specific information	Risks of attack on the collected, stored data and its transmission (both between sensor devices and services and users), and methods to ensure the confidentiality, authenticity and integrity of the collected and stored data.

Source: Caron et al. (2016: 8 & 12)

A countervailing possibility is that the increased risks of privacy will bring an advantage to those providers who demonstrate the highest standards of integrity and greatest data management competency (Weinberg et al. 2015: 616). Competition over privacy management can be an important way of raising standards (Competition & Markets Authority 2015). For this to occur, privacy protection needs to be important

to a business's reputation and brand value (House of Lords Select Committee on European Union 2016: 58). In the absence of direct competition over privacy management, it may be possible for intermediaries to develop a role as data managers on behalf of individual consumers (OECD 2015: 269).

Meanwhile, the Office of the Privacy Commissioner of Canada (2016: 16) argues that normal privacy principles should apply to the IoT, such as transparency over who collects what data for what purpose and the provision of 'opt out' choices without suffering any loss of service. It notes, however, some large barriers to applying privacy principles to the IoT.

- **Identifiability of IoT data**: aggregating, anonymising and de-identifying data do not assure privacy is protected (see also European Union Article 29 Data Protection Working Party (2014: 11). De-identified information can be matched against publicly available data to reveal personal identities (see MIT study), but this does depend on the de-identified data containing variables that can be linked to individuals. Strict rules about what constitutes de-identified data are required.

MIT study of de-identified data

Researchers at the Massachusetts Institute of Technology analysed anonymous credit-card transactions by 1.1 million people. Using four bits of secondary information, such as location or timing, the researchers identified the unique individual purchasing patterns of 90% of the people involved, even when the data were scrubbed of any names, account numbers or other obvious identifiers.

Researchers drew on bank records of purchases over a period of three months by shoppers at 10,000 stores. The data were de-identified but they retained a record of the day and place of purchase. After isolating a purchasing pattern, the research showed it was possible to find the name of the person in question by matching their activity against other publicly available information from social media sites that contain time and location data.

Source: de Montjoye et al. (2015)

- **Accountability in the land of machines**: it may be hard to attribute responsibility for privacy breaches. For example, data generated by a smart meter could variously be held the responsibility of the home owner benefiting from the device, the manufacturers or power companies that supplied the meter, the third party storing the data, the data processor or some combination of such parties. The OECD (2015: 271) also notes that the problem of diffuse accountability extends to regulatory agencies too. As an example, it cites how six separate public agencies regulate near-field communication in Australia (see ACMA 2013 for further discussion).

- **Transparency and the ethics of data collection**: devices on the IoT are expected to become part of the background environment, operating without active human intervention. This may be a challenge to individuals knowing what information is being collected, used, and disclosed for whose benefit. Transparency is needed to trace the source of privacy or security breaches, and to encourage good practice and the adherence to regulation (Weber and Weber 2010: 75).
- **He said, she said, 'It' said: access and correction rights**: privacy laws tend to rely on individuals initiating complaints, but identifying an obvious organisation to contact with a complaint is expected to be challenge in the case of the IoT.

Echoing these concerns expressed by the Privacy Commissioner in Canada, Martin (2013; 2016) questions the adequacy of 'notice and choice' as a mechanism for safeguarding privacy. This position is supported by economic analysis which can explain why people accommodate a loss of privacy against their preferences for privacy (see Appendix 2).

Notice and choice holds that as long as a company provides notice of its privacy practices, and people have some kind of choice about whether to provide the data or not, then privacy is sufficiently protected. Notice and choice provides the basis for consumers to maintain control of their personal data (Caron et al. 2016). Concern over the difficult of operating a notice and consent regime was expressed by informants to the recent UK enquiry into online platforms (House of Lords Select Committee on European Union 2016: 62):

> At present… few consumers read or fully understand privacy notices, which are normally embedded within a company's 'Terms and Conditions'.
>
> Citizens Advice said "approximately only a third of consumers' report that they read terms and conditions", but that "actually people are likely to be over-claiming"—according to the evidence of "actual time spent reading terms and conditions … the figure appears closer to 1%." The German Monopolies Commission confirmed that "the collection of personal data without users' explicit consent is likely to be not the exception, but in fact the rule."
>
> One problem with privacy notices is their length. Steve Wood, from the ICO, described many privacy notices as being "longer than Hamlet" while Professor Rodden said they were "as long as Othello" and Mr Alexander said they were "longer than the Declaration of Independence". They are, though, much less readable. Professor Rodden highlighted research undertaken by Research Councils UK showing that the language of privacy notices was "overly complex and difficult to read", and that they were "written to be understood and used in [a] US court rather than by ordinary consumers."

The inadequacy of existing notice and consent procedures is perhaps most pronounced in the case of devices connected to the IoT that are always on, theoretically requiring multiple separate notices and consents (OECD 2015: 265). Similarly, the Future of Privacy Forum (2013) argue that the lack meaningful user interfaces or screens on many connected devices poses a fundamental challenge to providing meaningful notice.

The Future of Privacy Forum proposes a new, 'use-focused' privacy regime in place of current privacy principles (as summarised in Table 6). This agenda is influenced by the claim that some relaxation of current privacy safeguards is justified to enable innovation. In particular, the proposed regime is designed to allow data to be collected for broader purposes than the present approach of restricting the right to collect personal data only in support of immediate interactions.

Table 6 Future of Privacy Forum contrast of old and new privacy principles

Principles informing current privacy laws and regulations	Principles informing a use-focused privacy regime for the IoT
• Notice - individuals should be provided with timely notice of how their data will be collected, used, and disclosed. • Choice - individuals should be given choices about whether and how their data will be used. • Data Minimization - organizations should seek to limit the amount of personal data they collect and that might be retained. • Purpose Specification - the purposes for which personal data are collected should be specified prior to or at the time of collection. • Use Limitation - personal data should only be used for those purposes specified prior to or at the time of collection.	• Use anonymized data when practical - risk of re-identification exists but can be minimised. • Respect the context in which personally identifiable information is collected. • Be transparent about data use - organisations should disclose how data inform decisions. • Automate accountability mechanisms - automated mechanisms could ensure conformance to machine readable policies. • Develop Codes of Conduct - Codes of conduct could establish frameworks that enable individuals to associate usage preferences with their connected devices. • Provide individuals with reasonable access to personally identifiable information.

Source: Summarised from Future of Privacy Forum (2013)

Somewhat in support of the Future of Privacy Forum's advocacy of more freedom to collect data, some benefits from a loss of privacy have been claimed (Weinberg et al. 2015: 616). People, for example, may find it harder to keep their lack of exercise and poor eating habits and behaviours hidden from their GP. Insurance companies may

be able to access information before settling claims that previously a claimant may have used to keep hidden (leaving doors unlocked or driving at speed).

Nonetheless, most comment appears to recognise the need for strengthened privacy protection. For example, the Information and Privacy Commissioner of Canada has promoted the idea of 'privacy by design'. This is endorsed by the EU Article 29 Data Protection Working Party (2014) which has also recommended the use of 'privacy impact assessments' and 'privacy by default'. In the UK, Ofcom (2015) has recommended efforts be made to simplify and standardise privacy terms and conditions. Among Ofcom's suggestions are that three levels of data sharing could be applied across all types of devices: unshared, shared only with service provider or shared with everyone.

Security and the IoT

A major data breach or cyber-attack is likely to have damaging consequences for public acceptance of the IoT. While not specifically a security issue of the IoT, the Superfish case is referred to as an example of how consumers do react when security risks become evident (Bailey 2015).

Superfish software and Lenovo PCs

Lenovo Group preinstalled its consumer laptops with ad-serving software known as Superfish. This made PCs vulnerable to hackers to access encrypted Web data and even online passwords. The software was preloaded on to computers with buyers given the opportunity of opting out when they started their computers for the first time. The option was not exercised by at least 250,000 customers. Checking by Microsoft suggested that even if an opt-out was exercised, Superfish appeared to remain on computers. On becoming aware of the problem, Lenovo removed the software but the incident was the cause of widespread adverse comment from the computer press.

Source: King (2015)

There is extensive comment on the security risks posed by the IoT, which has been heightened by recent illustrations of the ability to hack into connected vehicles (Campbell 2016) and children's toys (Kuchler 2015).

Cyber security experts in the US, for example, demonstrated it was possible for hackers to take remote control of a Jeep Cherokee. While this seems to confirm some fears, it should be noted that the simulated attack took two years to achieve by computer scientists who owned the Jeep and had access to its hardware before they gained entry to its systems remotely (Campbell 2016). In New Zealand, electricity consumers responding to a survey on 'smart home technology' identify the security of personal information as one of two major concerns (Ford and Peniamina 2016).

Britton (2016) identifies several inherent features of the IoT that underlie larger questions over data security.

- The IoT is connecting historic as well as new infrastructure. Upgrading this infrastructure will tend to require inter connected systems to be replaced rather than being open to incremental improvements. Inherited industrial control systems, for example, were not designed to be 'patched' or updated in the way a PC is.
- As consumers use more Internet-enabled devices and sensors, more and more points are open to attack.
- Many connected devices may not be capable of strong encryption because they lack both the necessary computing and battery power. Adding security capacity to IoT devices adds significantly to the cost and there is considerable cost sensitivity when the devices aim to reach millions of consumers.
- In an expanding IoT market, where time to market is critical in not being left behind, developers are not prioritising security.

Personal devices becoming a 'back door' to an organisation's' computer system is another security concern. Pritchard (2016) reports claims that data gathered from a person's fitness band could help outsiders to launch a cyber-attack against the user's employer organisation. For example, information on a fitness band may reveal when security personnel are on breaks, or when few people are in the office. Weber (2015: 626) expresses similar concerns with the AppleWatch, while acknowledging that steps have been taken to improve the security of the data it collects.

While security risks exist, the OECD (2015: 268) believes that cybersecurity policy making is at a turning point, with many countries now making it a national priority. In the USA, for example, the Federal Trade Commission (2015) has recently provided detailed guidance on steps that can be taken to address security concerns.

Data transparency

The importance of transparency for privacy protection was noted above. Two further related aspects of transparency have attracted comment: the application of algorithms to IoT data and the risks of discrimination.

Algorithms are applied to large data sets to turn data into information. Concern has been expressed about the difficulty of identifying the criteria programmed into algorithms (see, for example, the Electronic Privacy Information Centre campaign on algorithm transparency - https://epic.org/algorithmic-transparency).

Evidence presented to a government inquiry into online platforms in the UK referred to problems of accountability arising from the opaqueness of decisions made by data driven algorithms. The large number of parameters that are used by the algorithms is suggested to mean that even the engineers who constructed the system are often not

able to explain why the algorithms produce the results that they do (House of Lords Select Committee on European Union 2016: 49). Such an allegation arises in a commercial as well as a privacy context – see Facebook case.

Facebook algorithm shift hits media groups

SocialFlow, a platform used by publishers to post half a million stories to Facebook and other social media sites each month, estimates that stories posted to Facebook reached an average of 68,000 users in May, down from about 117,000 in January. The Financial Times reports Jim Anderson, SocialFlow chief executive as saying the fall shows Facebook has changed its algorithm.

"Facebook is constantly adjusting its algorithms up and down to tune the user experience," he said. "Back in the fourth quarter and through January, media companies were doing phenomenally well. Then Facebook made a change to the algorithm."

The SocialFlow chief executive also said: "These algorithms are pretty complicated. I'm not sure even Facebook engineers know their impact, they just have to measure and respond,"

Mr Anderson speculates that Facebook may have recalibrated the algorithm to prioritise posts from individuals to try to reward them for sharing more personal stories on the network, minimising feeds that feature several articles from the same news organisation consecutively and to prioritise video content.

Source: Financial Times 2 June 2016
http://www.ft.com/intl/cms/s/0/28cfe2a6-28eb-11e6-8b18-91555f2f4fde.html#axzz4AkkJ9GPX

The lack of transparency in how algorithms work raises questions about the ability to demonstrate compliance with regulation. Risk of discrimination consequently exists. Insurance companies, for instance, could disclose that they determine premiums solely by reviewing driving habits, location, driving history, and other permissible data categories. Privacy campaigners such as Electronic Privacy Information Centre argue that without disclosure of the criteria included in the data analysis, it is not possible to know that factors such as ethnicity, sexual orientation, and political preferences are not factored into the analysis.

The UK enquiry into Online Platforms recommended that platform providers such as Google should be required to provide more information about the construction of the algorithms that they use (House of Lords Select Committee on European Union 2016). They did not recommend enforcing fill disclosure, recognising that algorithms can include commercially important information.

Competition and the IoT

As an emerging technology at an early stage of development there are two extreme outcomes that may limit competition (Government Office for Science 2014: 16). One is that a single organisation or group could drive anti-competitive standards for the entire IoT, or at least a large segment of it. The other is that unless dominant standards emerge, it will be difficult for the IoT to achieve a framework that allows openness, interoperability and security.

A UK investigation into the competition effects of online platforms (which includes search engines, social networks and price comparison websites) identifies many ways in which dominance in a digital environment can act to limit competition (House of Lords Select Committee on European Union 2016). For example, online platforms have used their market power to engage in 'vertical integration/leverage, whereby a platform which serves as a marketplace also acts a retailer (paragraphs 142-144). This raises competition concerns because of the possibility that an online platform uses the information gathered through facilitating the marketplace to advantage the retail part of its business. Evidence given to the Committee by competition regulators and other experts indicates that such action is not unique to digital environments, can bring consumer benefits while having negative effects on competition and is controllable through existing competition regulation.

While the future competitive landscape of the IoT is unknown, risks to the protection of intellectual property are being viewed as a potential negative outcome of the IoT (Weber and Weber 2010: 21). Embedding digital devices in technology gives opportunity for criminals to gain access to that technology. Consequently, while the demonstration that it is possible for hackers to take control of a vehicle raised concerns for driver safety, the most likely motive for hacking vehicles is to steal intellectual property as well as personal data (Campbell 2016).

Governance and consumer protection

The lack of any international agreement covering privacy and data protection has been commented upon by legal experts (Weber and Weber 2010). While the IoT is global in scope, it is presently governed by national laws. Others express the view that the lack of governance that has characterised the emergence of the Internet is unlikely to change and should not change (for example, see Rueda-Sabater and Derosby 2011). However, there may be some areas where international agreement is required. One proposal is summarised in Table 7.

Table 7 A legal framework to provide international governance of the IoT

Governance area	Suggested scope of governance arrangements
Global application – the global distribution of services requires an international agreement.	Establishment of an international legal body that specialises in overseeing IoT non-compliance and accountability.

Ubiquity – mobility and multi-disciplinary use of sensors implies new legal challenges.	Sensors and other technology should be designed to ensure ability to adapt to changing environments and so that they are 'policy aware'. Technology needs to facilitate delegation of control to third parties.
Security – international standards should be adopted to ensure protection and privacy in all circumstances.	Rules for authorisation, trust and access control should be developed domain-by-domain. User-centric and context-centric policies should be developed, using predetermined privacy and security profiles.

Source: Adapted from Caron et al. (2016)

The OECD (2015: 270) identifies consumer protection and empowerment as a third necessary aspect of building trust in the IoT (along with privacy and security). Consumer protection is based upon adequate information disclosure, fair commercial practices including quality of service, and dispute resolution and redress. Ideally consumers are informed about how to use devices and related services, are able to determine the interoperability of devices and can identify who to turn to when problems with devices arise. The OECD (2015: 271) points to the UK Information Economy Council (https://www.digitalcatapultcentre.org.uk) as an helpful initiative seeking to address the interests of consumers in ways that should increase their confidence in the IOT.

Applications of the IoT

The IoT will bring different developments and opportunities according to the particular areas in which it is applied. In this sense while a common set of technologies lie behind the IoT, the impacts and potential concerns will vary with the precise area of application.

Ageing in place

The IoT has been linked to the concept of 'aging in place', allowing more people to stay at home rather than move into institutional facilities (Kenner 2008). Aging populations and pressures on health care systems are generating interest in surveillance technology as a viable alternative to ensure that people at risk, such as the disabled and elderly, can remain in their homes safely. Sensors worn on the body, for example, can interact with environmental sensors in the home to report falls or other mishaps to a caregiver. Similarly household technology can be activated by body sensors, for example linking body temperature to domestic heating systems.

Kenner (2008) warns that the context in which surveillance technology is introduced will influence its acceptability. It has also been noted that while the technology exists, the high cost of equipping homes with IoT devices is currently a substantial barrier to any widespread adoption (Gupta 2015).

The use of tracking devices to help manage people with dementia is sometimes given as one of the potential applications of the IoT. Research cautions against viewing surveillance technology as offering unambiguous benefits for people with dementia (Niemeijer et al. 2011; Zwijsen et al. 2012).

Zwijsen et al. (2012: 213) report that the Health Care Inspectorate in the Netherlands promotes the use of surveillance technology as a way to diminish the use of more severe means of restricting freedom. Surveillance technology in this context includes sensors (that can react to activity or inactivity) placed in clothing, beds, furniture and door surrounds, acoustic and GPS monitoring and electronic bracelets fitted with transponders to open doors. Based on the views of care professionals with experience of surveillance technology, Zwijsen et al. (2012) identify new challenges rather than clear cut improvements for either the people with dementia or the people who care for them.

Deployed to provide additional safety and freedom for people, care professionals identified four limitations in the use of surveillance technology:

- it is unable to prevent falling
- it cannot guarantee quick help,
- it does not always work properly
- and it could violate privacy (Zwijsen et al. 2012: 213).

Niemeijer et al. (2015) observed the use of surveillance technology (including tag and tracking systems and video surveillance) that allows dementia sufferers to move more freely around their residential care homes. This had various outcomes with some residents seeming to benefit while others experienced greater stress, as when the freedom of movement resulted in people getting lost or developing new behavioural routines that resulted in greater distress than when they were more confined. The study also observed how the greater freedom given to some residents could have adverse impacts on other residents, some of whom were judged not to be suited to the technology.

The use of the IoT for tracking people with dementia may appear helpful. In Japan, for example, over 10,000 people with dementia are reported missing from their homes or places of care annually. Japan's ageing population and a health care system that has not supported care in the community to the extent that exists in other countries are factors to be considered in explaining Japan's experience (Nakanishi and Nakashima 2014). Necklaces and shoes with GPS tracking are available, but their usefulness is in managing people receiving care.

Connected vehicles

Transport is expected to be one of the areas transformed by the IoT. Fully autonomous vehicles could ultimately be integrated into a transport system of smart roads, traffic lights, signs, streetlights and parking. In the UK, a review of a review of the Highway Code has allowed autonomous transport to be trialled on public

highways, with trials of autonomous road-going cars and public transport 'pods' underway (Sharman 2015). Possibilities for the future include combining location data with projected routes to simulate a complete journey congestion map. Prior insight into where congestion is expected might then be used to guide vehicles on to alternative routes or alter journey times (Miller 2015: 270-271). Using connected cars to collect data to inform infrastructure planning, as with Boston's 'Street Bump' app.

The UK Government Office for Science (2014: 24) identifies 'complex questions' over regulation, ethics, liability and social norms to be resolved if the connected car is to become a reality. These issues are greatest in the case of driverless cars. How is an autonomous vehicle to be programmed, for example, to choose between multiple negative outcomes if it is an accident situation? As well as legislation and liability questions, Sharman (2015) reports that the development of driverless cars will depend on the end of private ownership, with cars of the future expected to be shared or operated as public fleets.

Immediately, something that is being enabled by the IoT is the collection of mileage and driving behaviour data (Derikx et al. 2016). It is envisaged that this will see the development of traffic safety services, vehicle diagnostics, preventive maintenance and advanced real time navigation support (Leminen et al. 2012).

Derikx et al. (2016) examine if and how privacy concerns for connected car services can be compensated financially using the example of usage-based insurance services. They indicate that usage-based insurance services are starting to be introduced utilising GPS-data and motion sensors to measure aspects of driving behaviour. In an experimental study (based on 60 respondents), they find that consumers prefer their current insurance products to usage-based car insurance. A minor financial compensation, however, is sufficient to shift this preference and make usage-based insurance attractive. The study finds that consumers find privacy of road driving behaviour more valuable than information about locations visited and distance travelled.

Retail environments

The Office of the Privacy Commissioner of Canada (2016: 8) provides some examples of passive and active interaction that generates data for retail analytics, further differentiating between data collected in-store and outside an individual store (Table 8).

Table 8 Examples of data sources for retail analytics and marketing collected through passive and active means.

	In-store	Outside of store
Passive observation	• Location tracking via short-range radio • Short-term behaviour analysis	• Location tracking via medium and long-range radio • Neighbourhood-level tracking

	• Video cameras used to analyse customer traffic flows • Facial detection and analysis to customise digital signs and ads	• Long-term behaviour analysis
Active interaction	• Downloading an app to receive coupons when in-store • Connecting to a free Wi-Fi service • Completing a NFC-enabled transaction (eg. payment via a smartphone)	• Creating a digital perimeter around a store so coupons can be delivered when a potential customer approaches • When an individual walks by a competitor's store, post coupons to their mobile device to draw them to their own store

Reflecting on the capacity for monitoring consumer behaviour with both passive observation and active intervention, Kang and Cuff (2005) have identified two scenarios for the future of the retail shopping environment, assuming no effective action is taken to enable individuals to protect their privacy: smooth mall and friction mall (Table 7).

> ***Smooth mall***: through the IoT retailers and managers of shopping malls have extensive capacity to profile consumers. This insight is used to limit or discourage entry into the mall or some part of the mall, for example an area devoted to upmarket stores. Post entry to the mall, the insight into a visitor's behaviour and preferences is exploited to encourage mall visitors into a 'passive, consumption-only' mindset.
>
> ***Friction mall***: emphasising the capacity to deliver tailored information in real-time, shopping experiences in the IoT-enabled mall, shoppers may be open to a proliferation of competing agendas seeking to influence purchasing decisions. Scanning the electronic code on a product of interest brings forth a flurry of counter-information: environmental groups alert the would-be purchaser to coffee's role in deforestation; the neighbouring store offers the same product at a lower price; a competing manufacturer sends an advertisement for its brand with a coupon for a free coffee at a nearby coffee shop.

Kang and Cuff (2005) use these scenarios to advocate for strong controls over the collection and use of personal data. In the USA, the Electronic Privacy Information Centre (www.epic.org/privacy/internet/iot/) makes reference to the analysis in its campaign for greater privacy protection.

Smart homes

A 'smart home' is fitted or equipped with a range of interconnected sensors to read external elements such as light, temperature, motion, moisture of systems such as heating, lighting, security and to control home appliances. Smart home technology may be automated, monitored and controlled through a computer or smart phone, including remotely. The smart home has potential to provide occupants with sophisticated information about the state of their home, and to provide increased capacity to control their home technology.

The Privacy Commissioner of Canada (2016: 12) quotes research that anticipates three likely patterns in the development of smart home technology.

- A fully decentralised smart home where each device is autonomous and which makes use of the existing home network to the Internet and transmits data to the service provider in the cloud.
- A home with an enabled local connectivity between smart devices, without the use of connection to cloud services and without a central getaway.
- A home with a central hub where a central software system—and accessible from one central device—coordinates all the smart devices and integrates their services to create added-value.

In New Zealand, few homes have smart home technology installed but there is reported to be high interest in devices such as smart thermostats, smart appliances, smart plugs, and smart lights (Ford and Peniamina 2016).

A note of caution from the OECD (2015), is that the drive to adopt smart home technologies will be the desire to make life simpler. Yet they note that even one device, such as a smart heating controller, can be complex to programme and manage. They suggest anyone with several devices may need guidance on ways to access and use them. The full functionality will also require the ability to control their smart home devices from any Internet connection, which will require a high level of service security and interoperability.

The Privacy Commissioner of Canada (2016) identifies some aspects of the smart home that may become sources of concern:

- Smart meters based on two-way communication between the home and energy provider, can include the capacity of the energy provider to adjust home energy consumption to suit overall demand and supply conditions.
- Home security systems approved by insurance companies for lower insurance premiums, can require that security cameras are visible or promotional material is displayed advertising the surveillance system in place. Small covert cameras can record anyone who comes within distance, whether they be a neighbour, visitor, courier, tradesperson or someone with criminal intent.

- Smart TVs seamlessly move between entertainment, social media and web browsing, so the capability to channel carefully targeted advertising into the home increases.

Implications for research

International technology consultants Gartner are frequently quoted for their claim that 2014 was the peak year of inflated expectations about the IoT. While expectations are high, this can also mean that concerns over the possible negative effects may also be high. The absence of any proven business models for achieving profitability is further reason for exercising caution about the speed and scale of innovation.

Based on the issues attracting attention overseas, a number of areas merit investigation in New Zealand.

- How well positioned is New Zealand to provide the infrastructure to support the IoT? Does a roadmap for an IoT infrastructure need to be developed, and if so who should be involved in developing that roadmap?
- Is there a role for government to act as a strategic customer for the IOT, using its position to help set best practices or to facilitate demonstrator projects?
- What part is and should New Zealand be playing in helping to develop standards that can facilitate interoperability and openness to new business start-ups?
- Is New Zealand adequately recognising and responding to the privacy and security concerns expressed around the IoT? Is there a need to bring relevant agencies together to develop a strategy for ensuring best practices with respect to privacy and security are embedded within New Zealand's IoT?
- How well placed is New Zealand to manage the privacy concerns arising from the IoT? Is there support for a shift in the principles governing the protection of privacy to facilitate innovation and development of the IoT?
- How can competition over data privacy and security be encouraged so as to maximise consumer ability to discriminate providers according to their privacy performance?
- Is there a need for regulations to be reviewed to facilitate the operation of more types of autonomous machine, such as driverless cars?

Appendix 1 – Technology and the IoT

Appendix Table 1 identifies some of the main technologies involved in the IoT. The connections creating the IoT may send data for processing to centralised servers or involve direct machine-to-machine communication. The OECD (2015: 244) adds cloud computing and big data analytics to the enabling technologies, noting that this brings in the possibility of improved machine learning applications and artificial intelligence.

The quantity of devices in the IoT will dwarf those linked to the traditional internet. Alternative protocols, tools and techniques are needed to accommodate the massive explosion of connectivity, particular where the things connected are comparatively low value objects that are required to communicate data intermittently (daCosta 2013: 5).

Appendix Table 1 Technologies supporting the Internet of Things

RFID	Radio-frequency identification used mainly for tracking and tracing objects.
Near-field communications (NFC)	Adaptation of RFID providing short-range, low power wireless to transfer small amounts of data between devices.
Machine-to-machine communications (M2M)	A term used to distinguish the application of the IoT for industrial, business and commercial applications from the consumer applications of the IoT.
Wireless sensors	Different to RFID in that they measure features of the physical environment, such as pressure, heat and humidity.
Actuators	Convert information or energy from sensors into action by transmitting it to another power mechanism or system, such as heating or cooling a room. Can operate without human intervention.

Source: Office of the Privacy Commissioner of Canada (2016: 3-4).

A wide variety of technologies are identified as part of the emerging IoT. Appendix Table 2 categorises IoT devices into six main areas of application: wearables, building and home automation, smart cities, health care, smart manufacturing, and automotive. An EU-based survey suggests that IoT technologies have potential to be applied across multiple sectors but that implementation is developing fastest in three areas (Mazhelis et al. 2013):

- Automotive/Transportation: in-vehicle infotainment, eCall, parking meters, information sharing about road conditions and traffic density, road pricing, toll collection, taxation, pay as you drive (PAYD) car insurance;
- Digital home: (home) consumer electronics, home automation, automated meter reading (AMR), residential security;
- Healthcare: monitoring solutions to support wellness, prevention, diagnostics or treatment services.

Appendix Table 2 Classifying IoT devices by the area of application

Wearables • Entertainment • Fitness • Smart watch • Location and tracking	**Health care** • Remote monitoring • Ambulance telemetry • Drug tracking • Hospital asset tracking • Access control • Predictive maintenance
Building and home automation • Access control • Light and temperature control • Energy optimisation • Predictive maintenance • Connected appliances	**Smart manufacturing** • Flow optimisation • Real-time inventory • Asset tracking • Employee safety • Predictive maintenance • Firmware updates
Smart cities • Residential e-meters • Smart street lights • Pipeline leak detection • Traffic control • Surveillance cameras • Centralised and integrated system control	**Automotive** • Infotainment • Wire replacement • Telemetry • Predictive maintenance • Car to car, and car to infrastructure

Source: Weinberg et al. (2015) adapted from Texas Instruments (2014)

Data collection mechanisms

The UK Competition & Markets Authority (2015: 31) identifies two main ways that individuals declare information about themselves.

- Actively declared data – consumers voluntarily declare information about themselves when, for example, registering for services, purchasing products or services, entering competitions or participating in surveys. Individuals know they are submitting data, but they may not always know the uses to which it might be put.

- Passively supplied (observed) data – car number plates, computers, mobile phones, tablets and computer mice are harvested for various forms of so-called 'exhaust' data.

The CMA (2015) identifies a number of specific ways that the capacity for passively harvesting personal data is growing as an outcome of the IoT (Appendix Table 3).

Appendix Table 3 Examples of devices collecting and transmitting consumer data

Mobile phone and tablet location tracking	Retailers may be able to pick up IDs unique to owners' devices and track them within and outside stores. Some apps ask device owners to share their location data, and this information may be shared with other parties. Where consumers provide data to use Wi-Fi hotspots, this may be shared with third parties for marketing but also to track their in-store location.
Facial recognition	Cameras and specialist software enable stores and advertisers to target people with particular age and gender characteristics. Face-scanning technology can target advertisements to customers at the checkout.
Home automation ('domotics') and 'smart devices'	IoT devices such as smoke alarms, lights, washing machines, fridges, ovens and thermostats can be controlled online – for example, so that home owners can change settings while away, or to place orders. Some smart TVs may share information on people's viewing that can be used to target advertising
Wearable technology and the 'quantifiable self'	Wearable devices such as watches can monitor health; glasses can record images and provide real-time location-based information. The data collected by wearable devices can be used by third parties to monitor and analyse individuals' health indicators and offer tailored advice.

Source: UK Competition & Markets Authority (2015: 33-34)

Caron et al. (2016) summarise potential areas of application that may benefit from the IoT, according to the types of sensors and typical data each sensor may record (Appendix Table 3).

Appendix Table 3 Possible areas of impact from the IoT according to the type of sensor and data recorded

Type of sensor	Recorded data	Potential area of application
Camera (CCTV)	Movement, facial recognition	Crime investigation
Smartwatch	Vital signs, movement, voice recordings	Healthcare
Google Glass	Surroundings, movements	Improved marketing interactions
Building sensor	Movement, heat, consumption (water, power, internet)	Energy industry
Smartphone	Call history, location, movement, internet/app activity	Crime investigation, fraud
Goods packaging	Tracking delivery, quality control, real-time inventory	Retail industry
Human implants	Tracking blood pressure, location, heartbeat	Healthcare
Vehicle	Movement, driver behaviour, fatigue/alcohol, traffic reduction	Consumption savings, accident prevention

Source: Caron et al. (2016) based on Stanford (2003) and Atzori et al. (2010)

Appendix 2 Economics of privacy and the IoT

Economic theory has been drawn upon to explain why it may be possible for the IoT to develop with low standards of privacy protection. Drawing on transaction cost theory, Martin (2013) gives three reasons for claiming that 'notice and choice' provides little privacy protection (Appendix Table 5).

Appendix Table 5 Reasons why 'notice and choice' does not protect privacy in the IoT

Information asymmetries	Information asymmetries exist when one party has information about a transaction that is not available to another. In an online environment, capturing a complicated data flow that can involve data aggregators, ad networks, third party tracking companies as well as a primary website/device in a succinct and comprehensible privacy statement creates a knowledge imbalance, even if individuals read a privacy notice. A 'transparency paradox' exists where the more information that is revealed the more incomprehensible are the statements and less likely authentic consent is given (see also House of Lords Select Committee on European Union 2016).
Enforcement	In an online context, users are at a disadvantage to be able to identify: (1) a violation of privacy; (2) the responsible party; (3) the steps to fix a violation.
Uncertainty	The online environment is uncertain in the sense that technology is still under development. This introduces the possibility of as yet unknown mechanisms through which information may be obtained, combined and leaked to third parties. The general trajectory has been that successive innovations have brought increasingly persistent tracking mechanisms.

Source: Martin (2013)

With privacy at risk, joining the IoT requires people to trade away their privacy rights for the benefits obtained from using IoT devices (Bailey 2015). Some people using IoT devices may be ignorant of the privacy risk (a possibility canvassed in detail by Peppet 2014). Privacy trading involves people who recognise that privacy risks exist, but who nonetheless make use of IoT devices because of the immediate benefits obtained. Drawing on behaviour economics, Bailey (2015) offers two main reasons why people engage in privacy trading:

- ***Unrealistic optimism***: behavioural economics has identified how people tend to misjudge their ability to avoid risk. Bailey (2015: 1036) suggests that this extends to a tendency for people to think that they are less at risk of being affected by a breach of their privacy than the average person is. Bailey also refers to the 'availability heuristic' as a reason for discounting privacy risks

when engaging with IoT devices. As there is currently no widespread media coverage of privacy breaches, people do not have available information that would adjust their risk assessment.

- ***Hyperbolic discounting***: a principle of behavioural economics is that people are more impatient with regard to the near future than they are about the far future. To illustrate, many people prefer $100 now to $110 in a day, but few people prefer $100 in 30 days to $110 in 31 days. This is called hyperbolic discounting (in contrast to exponential discounting) because of the way that people's evaluation of delayed consequences is affected by the length of the time delay. Bailey (2015: 1040) gives the example of a person purchasing a wearable fitness device to illustrate how hyperbolic discounting applies to the IoT. The purchaser may be concerned with the privacy of the data collected by the device, but their immediate preference is the convenience of wearing the device. They may figure that after six months, having refined their training regime with the aid of the device they will then cease to use it. When six months are up, however, the convenience of using the device once again overrides their long term wishes and they opt to continue using it.

Bailey (2015: 1054) argues that since behavioural biases can explain why people use IoT devices, regulatory intervention to protect privacy should be designed to also correct the biases.

- To counter over optimism, consumers need to be advised of the potential for privacy loss (and how it may occur) and this should be reinforced by a vivid anecdote about a person who has been affected by a privacy breach.
- To counter hyperbolic discounting, the default rule could be changed from the present situation where consumers are required to opt-out if they do not wish to accept a provider's terms and conditions, to an opt-in requirement. An opt-in requirement would mean that providers of IoT devices would need to obtain explicit consent from individuals before collecting, using or exchanging information about them.

References

Anderson, J. and Rainie, L. (2014) The Internet of Things Will Thrive by 2025. Pew Research Centre. Available at: www.pewresearch.org

Article 29 Data Protection Working Party (2014) Opinion 8/2014 on the recent developments on the Internet of Things. September 2014.

Atzori L, Iera A, and Morabito G. (2010) The internet of things: a survey. Computer Network 54:2787–2805.

Australian Communications and Media Authority (ACMA) (2013) Near-field communication. Emerging issues in Media and Communications. Occasional Paper 2. Canberra: ACMA.

Bailey, M. (2015) Seduction by technology: why consumers opt out of privacy by buying into the Internet of Things. Texas Law Review 94: 1023-1054.

Britton, K. (2016) Handling privacy and security in the Internet of Things. Journal of Internet Law April: 3-7.

Campbell, P. (2016) Data-hungry cyber hackers turn gaze to connected autos. Financial Times May 11

Caron, X., Bosua,R., Maynard,S. and Ahmad, A. (2016) The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective. Computer Law & Security Review 32: 4–15.

Competition & Markets Authority (2015) The commercial use of consumer data: report on the CMA's call for information. CMA38. London: CMA.

Da Costa, F. (2013) Rethinking the internet of things. A scalable approach to connecting everything. Apress Media: New York.

de Montjoye, Y., Radaelli, L. , Singh, V. and Pentland, A. (2015) Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 30 January: 536-539.

Derikx, S., de Reuver, M. and Kroesen, M. (2016) Can privacy concerns for insurance of connected cars be compensated? Electronic Markets 26:73–81.

Federal Trade Commission (2015) Careful Connections: Building Security in the Internet of Things. FTC Staff Report. Available at: https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

Ford, R. and Peniamina, R. (2016) Smart Homes: What New Zealanders think, have, and want. Dunedin, NZ: Centre for Sustainability, University of Otago.

Future of Privacy Forum (2013) A new privacy paradigm for the "Internet of Things." https://fpf.org/2013/11/19/fpf-releases-a-new-privacy-paradigm-for-the-internet-of-things

Greengard, S. (2015) The internet of things. Cambridge MA: MIT Press.

Gupta, S. (2015) For the disabled, smart homes are home sweet home. Fortune February 1.

House of Lords Select Committee on European Union (2016) Online Platforms and the Digital Single Market. HL Paper 129. London: House of Lords

Kenner, A. (2008) Securing the elderly body: Dementia, surveillance, and the politics of "aging in place". Surveillance & Society 5(3): 252-269.

King, B. (2015) Lenovo's Superfish fallout: Can we forgive and forget? Fortune March 5. Available at: http://fortune.com/2015/03/05/lenovos-superfish-fallout-can-we-forgive-and-forget/

Kuchler, H. (2015) VTech hack puts spotlight on vulnerabilities of connected toys. Financial Times December 1.

Leminen, S., Westerlund, M., Rajahonka, M., Siuruainen, R. (2012). Towards IoT ecosystems and business models. Internet of Things, Smart Spaces, and Next Generation Networking (pp. 15–26): Dordrecht: Springer.

Martin, K. (2013) Transaction costs, privacy, and trust: the laudable goals and ultimate failure of notice and choice to respect privacy online. First Monday 18(12). http://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/4838/3802

Martin, K. (2016) Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop? The Information Society 32(1): 51–63

Mazhelis, O., Warma, H. et al. (2013) Internet -of -Things Market, Value Networks, and Business Models: State of the Art Report. Deliverable D5.1.2 TIVIT Internet of Things Programme, Jyväskylä University, Finland

Miller, M. (2015) The internet of things: How smart TVs, smart cars, smart homes, and smart cities are changing the world. Indianapolis: QUE Publishing/Pearson.

Nakanishi, M. and Nakashima, T. (2014) Features of the Japanese national dementia strategy in comparison with international dementia policies: How should a national dementia policy interact with the public health- and social-care systems? Alzheimer's & Dementia 10: 468–476.

Niemeijer, A., Frederiks, B., Depla, M., Legemaate, J. , Eefsting, J. and Hertogh, C. (2011) The ideal application of surveillance technology in residential care for people with dementia. Journal of Medical Ethics 37:303-310.

Niemeijer, A., Depla, M., Frederiks, B. and Hertogh, C. (2015) The experiences of people with dementia and intellectual disabilities with surveillance technologies in residential care. Nursing Ethics 22(3): 307–320.

OECD. (2015) Emerging issues: The Internet of Things. In OECD Digital Economy Outlook 2015. Paris: OECD Publishing.

Ofcom (2015) Promoting investment and innovation in the Internet of Things: Summary of responses and next steps. London:Ofcom.

Office of the Privacy Commissioner of Canada (2016) The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments. Research paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada.

Palmer, M. (2015) The internet of things: expect the spectacular — but just not yet. Financial Times 27 January 2015.

Peppet, S. (2014) Regulating the Internet of Things: First steps toward managing discrimination, privacy, security, and consent. Texas Law Review 93: 85-176.

Pritchard, S (2016) Internet of things: humble lightbulbs could become a form of attack. Financial Times March 16

Rueda-Sabater, E. and Derosby, D. (2011) The evolving Internet in 2025: four scenarios. Strategy & Leadership 39(1): 32 – 38.

Sharman, A. (2015) UK aims to be destination of choice for driverless car testing. Financial Times June 18

Stanford, V. (2003) Pervasive computing goes the last hundred feet with RFID systems. Pervasive Computing IEEE 2(2):9–14.

Texas Instruments. (2014). Application areas for the Internet of Things. Available at: http://www.ti.com/ww/en/internet_of_things/iot-applications.html

Weber, R. (2015) Internet of things: Privacy issues revisited. Computer Law & Security Review 31: 618–627.

Weber, R. and Weber, R. (2010) Internet of Things: Legal perspectives. Berling: Springer-Verlag.

Weinberg, B, Milne, G., Andonova, Y. and Hajjat, F. (2015) Internet of things: Convenience vs. privacy and secrecy. Business Horizons 58: 615—624.

UK Competition & Markets Authority (2015) The commercial use of consumer data. Report on the CMA's call for information. CMA38. London: CMA.

Government Office for Science (2014) The Internet of Things: Making the most of the second digital revolution. A report by the UK Chief Scientific Adviser. London: The Government Office for Science.

UK Parliamentary Library (2015) House of Commons briefs: The Internet of Things: Key issues for the 2015 Parliament. Available at http://www.parliament.uk/business/publications/research/key-issues-parliament-2015/technology/internet-of-things/

Zwijsen,S., Depla M., Niemeijer, A., Francke, A. and Hertogh, C. (2012) Surveillance technology: An alternative to physical restraints? A qualitative study among professionals working in nursing homes for people with dementia. International Journal of Nursing Studies 49: 212–219.