IoT: who stops Dr Jekyll from becoming Mr Hyde?

Principal, Data Synergies
Chair of IoTAA Data work stream[1]

Introduction

All new consumer focussed, data driven services – whether social networking, search engines, sharing economy, price comparison and IoT services - raise novel consumer protection concerns that need to be addressed.

Key concerns include:

- unanticipated uses and disclosures of consumer data,
- ensuring privacy and security by design and default,
- mitigating risks of security vulnerabilities and unanticipated and unauthorised uses,
- ensuring that buyers and users of IoT services understand vulnerabilities inherent to devices and services and their responsibilities in mitigating those risks.

These concerns should not be addressed through risk shifting, or through 'papering the way to compliance', or through 'washing' privacy/ethics/consumer protection evaluation that does not properly address the concerns.

In particular, the benefits of IoT services will not be safely realised unless we ensure that IoT device and service suppliers, buyers (whether Government agencies, businesses or consumers), users and other affected individuals (such as those humans observed or otherwise affected) understand 'who-is-doing-what' and 'who-is-responsible-for-doing-what'.

IoT services will only be safe, reliable and predictable if we ensure that allocation of respective responsibilities of suppliers, buyers, users and other affected individuals is fair, transparent and understood.

There already is wide diversity of IoT applications, of IoT deployment architectures and scenarios for implementation. And IoT devices and services are already heterogeneous, with capabilities dynamically evolving through new release of new products, through 'in-the-field' over–the-air (OTA) upgrades of existing IoT devices, and through new interfaces and interworking. What is understood today about a device in use may be outdated tomorrow, frequently without direct intervention by a user, and often without a user understanding the full implications of new features, functionality or interworking. There is also significant diversity in extent of personalisation and intimacy of observations IoT applications. This diversity means that generalisations as to IoT issues and concerns, and particularly as to privacy impact, are potentially misleading. That noted, it is fair to suggest that a number of common features of IoT devices and IoT services will have the effect that consumer-related

[1] Peter Leonard is a data, content and technology business consultant and lawyer and principal of Data Synergies. Peter is a Professor of Practice at UNSW Business School. Peter was a founding partner of Gilbert + Tobin and following his retirement as a partner in 2017 he continues to assist Gilbert + Tobin as a consultant. Peter chairs the IoTAA's Data work stream. The IoT Alliance (www.iot.org.au) is Australia's peak IoT body, bringing together industry government and regulators to address issues affecting IoT adoption and implementation, chairs the Law Society of New South Wales' Privacy and Communications Committee and the Australian Computer Society's Artificial Intelligence and Ethics Technical Committee.

issues are likely to be magnified for many business to consumer (**B2C**) IoT services as compared to many other consumer focussed, data driven services.[2]

This paper explores a number of concerns as to IoT devices and services, also noting that some of these concerns are being addressed through collaborative efforts in Australia to address such concerns, including the IoT Alliance Australia's (**IoTAA's**):

- [draft] *IoT Reference Framework,*
- *Internet of Things Platform Selection Guideline*,
- *Internet of Things Security Guideline*,
- *Good Data Practice Guide for Business to Consumer B2C IoT Services for Australia*, [3]
- [draft] *IoT Security Trust Mark.*

At the outset, it should be noted note that many consumer-related concerns as to B2C IoT devices and services arise through the combination of:

- suppliers 'learning by doing' in a novel business space – compare social networking services, where many issues about algorithmic driven 'funnelling effect' and political and social manipulation were only identified over five years after the first phase of user take-up of those services;
- unfamiliarity with consumers as to ways in which consumers can manage and mitigate risks and vulnerabilities, including of over-reliance, of implementation and use by consumers of IoT devices and services.

In other words, some of the issues arise because of **novelty of the IoT sector**. Novelty inevitably means the predictions as to what will be problems, and what won't, will inevitably be incorrect - at least in part. In such circumstances, a good first step is to promote a discussion between suppliers and consumers as to what worries consumers. An important part of this is discussion about 'social licence'. When people trust that data about them will be used only as they understand and agree, and accept that they understand risks of that enough value will be created and fairly distributed, there is 'social licence'.

Unfortunately Australia has been slow in initiating a broad-ranging discussion between government, industry and consumers as to social licence for uses of consumer data. The traditional Australian approach (although never formally acknowledged as such) is that government, commissioners and regulators know best, and regulation should head-off problems before they occur. By contrast, New Zealand has just ended the first phase of a world-leading initiative, the Data Futures Partnership[4], for engaging with citizens what a data-driven society might look like, and engaging with their concerns about implications of pervasive data collection and data dependency. That work has included an interesting study

[2] See further Richard Kemp, Legal Aspects of the Internet of Things, June 2017 http://www.kempitlaw.com/legal-aspects-of-the-internet-of-things/, Peter Leonard, AI Challenges and the Law: Being smart enough to boss around smart devices, September 2018 https://www.scl.org/articles/10295-ai-challenges-and-the-law-being-smart-enough-to-boss-around-smart-devices-and-ai, Peter Leonard and Toby Walsh, #MeToo for AI? Could Cambridge Analytica happen again? May2018, https://www.scl.org/articles/10210-metoo-for-ai-could-cambridge-analytica-happen-again, Peter Leonard, The Internet of Things (aka The Internet of Everything): What Is It About and Who Should Care, August 2016 https://www.gtlaw.com.au/insights/internet-things-aka-internet-everything-what-it-about-and-who-should-care,

[3] For more on the IoT Alliance Australia, see www.iot.org.au. The Guide is available at that site through www.iot.org.au/resources.

[4] See further http://datafutures.co.nz/ and materials linked through that site.

of social licence and IoT[5], and publication of a guide to developing trust of citizens and users of data-driven services.

1 IoT 1.01: a brief introduction to IoT services and IoT devices

(a) What are IoT services and IoT devices?

At its most basic, the IoT is the concept of connecting any device with an 'on' and 'off' switch to the Internet and/or to other devices. IoT devices may be any device capable of connection: hence the alternative moniker for the IoT of *the Internet of Everything*. More formally, the IoT is defined as infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.

Consumer IoT devices include everything from connected vehicles, connected TVs, connected toys, smartphones (often doubling as control (actuator) devices for IoT services and reporting devices as to data outputs from IoT sensors), to energy meters, security monitoring, thermostats, kettles, swimming pool filters, washing machines, headphones, lamps, wearable devices and so on.

Some IoT consumer applications provide consumers with information that enables the consumer to make actionable decisions based upon the analysed information. For example, 'smart home' applications to turn on an air-conditioner, to turn off a pool filter or to order chemicals required to treat a swimming pool. Other applications may fully control and self-adjust in response to a particular environment without any active consumer intervention: for example, smart home applications that respond to an extreme weather event by automatically activating sprinklers, closing curtains, turning off non-essential electrical appliances and turning on an air-conditioner that services a pet area.

Although there are many different types of IoT applications and services, a key element of many IoT services is incorporation of sensor devices and actuator devices. Sensors may be passive devices that monitor and report over the Internet as to conditions in a particular environment, or active devices that change conditions in that environment.

Increasingly over time, IoT services will be machine-to-machine, rather than human-to-machine. Absence of direct human intervention may lead to concerns as to awareness of affected individuals in relation to ongoing collection and handling of personal information about them in the course of provision of such services. This may particularly be the case where there affected individual is not directly involved in ordering up or commissioning installation of the IoT service. For example, an IoT security monitoring application installed in a rental apartment may have been commissioned by the landlord, and the tenant and any invitee to the apartment may be unaware of the terms of provision of the IoT security service and as to any collection and handling of information about them that is enabled by that application.

(b) Why are we suddenly hearing so much about IoT? Is it hype?

Technological factors are converging to escalate the pace of IoT deployment.

[5] See Perry, P. (July 2016) "Social Licence and the Internet of Things, A Report for the Data Futures Partnership", available at http://datafutures.co.nz/assets/Uploads/FINAL-Social-licence-and-the-IoT-literature-review.pdf, and New Zealand Data Futures Partnership "A Path to Social Licence, Guidelines for Trusted Data Use" (August 2017), available at https://trusteddata.co.nz/wp-content/uploads/2017/08/Background-Trusted-Data.pdf.

These factors include:

- as to sensors, rapid reductions in cost consumption coupled with improvements in capacity, durability, robustness and power efficiency;
- improvements in communications technologies between sensors and hubs and control devices, including 'meshed networks' and other improvements in bandwidth utilisation and reliability;
- improvements in encryption and other technologies to protect security of data both at rest and in transit;
- rapid uptake of smartphones, enabling near ubiquity of availability (subject to mobile network and wifi coverage) of a relatively low cost and globally standardised device which enables insights to be delivered to users and the smartphone used as an actuator device;
- rollout of cloud based data warehouses and cloud based analytics platform services, enabling interconnectivity of services and low cost set-up and tear-down of data sources and analytics capabilities; and
- rollout of broadband and narrowband networks and IoT platforms and hub devices that support third party IoT services. Many low cost IoT smart home applications require access to an IoT hub device, such as a Nest™ device, provisioned by a third party such as a consumer.

IoT is over-hyped, but it is real, and IoT deployment and take-up still accelerating.

2 Risks and challenges of IoT

The opportunities afforded by IoT come with attendant risks and challenges, many novel and requiring development of new business models, law and new forms of contract.

Rapid uptake of IoT largely reflects the many benefits that smart devices bring to our lives. And rapid uptake is not of itself a problem, if user awareness of the capabilities and limitations of such devices keeps pace with deployment of devices and changes in features and functionality of those devices. But the deployment and use of new capabilities is increasingly opaque. One important change is that the capabilities are often not controlled by the affected individual – or as the GDPR more clearly expresses it, 'the data subject'. Our current thinking as to appropriate privacy settings and safeguards has focussed upon user-controlled personal access devices such as smartphones and user-initiated activity in use of social networking services, internet search and 'acceptance' of cookies and online tracking identifiers behavioural advertising. Our regulatory response has been:

- to require higher transparency of what providers of services are doing,
- to require more convenient privacy settings,
- to cajole online service providers to improve consumer trust,
- to name and shame (and sometimes fine) service providers that significantly transgress.

This approach might be sufficient in an adult, allegedly user-controlled, world that is based upon a 'transparency and contract' view of privacy. In this world, many citizens apparently take the view that you only have yourself to blame if you don't bother to set appropriate settings that are made available to you, that you could have elected to set if only you had bothered to find and read the explanation of how to do so.

This is not a reasonable view of our new 'smart' world.

Our smart world will soon be dominated by devices:

- where settings are determined by others,
- where settings are not as readily seen or understood,
- where vulnerabilities in data security are common, and
- where some users don't know or forget that the device is there and in use, while other users become overly dependent upon those devices operating reliably in conditions for which the device is not designed, or in operating environments where the device is simply not consistently reliable.

As these devices are increasingly given important responsibilities for control and actuation – to autonomously cause other devices to be activated or deactivated in certain conditions – the risks of over-reliance, or of being lulled to sleep as to shortcomings or limitations, or being commanded by malicious actors, quietly increase.

Because we don't see these semi or fully autonomous agents as robots-that-look-like-robots, we don't interrogate these capabilities or apply the same level of scrutiny or oversight as we are now doing for more distant AI applications such as robots-that-look-like-robots or self-driving cars. So we recognise these risks, to be addressed with some haste as we hurtle towards a more manifestly AI world, but still future risks. This is a mistake.

3 Allocating Responsibility

So how do we translate such homespun thinking into a concrete path for development of data and consumer law and regulation?

There are a few reasons why this is not easy.

Privacy and security challenges of IoT services are illustrated by the September 2016 study of GPEN (the Global Privacy Enforcement Network), a grouping of national privacy authorities.[6] The GPEN report found that about two thirds of devices surveyed failed to explain adequately to customers how their personal information was collected, used, stored and disclosed. In particular, almost three quarters failed to show it could be deleted off the device. In just over one third of cases, the devices did not include easily accessible contact details for the provider.

[6] See "2016 GPEN Privacy Sweep, Internet of Things: Participating Authorities' Press Releases" at https://www.privacyenforcement.net/node/717; also OAIC (September 23, 2016) "Privacy Commissioners reveal the hidden risks of the Internet of Things" https://www.oaic.gov.au/media-and-speeches/media-releases/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things.

Similar concerns have been detailed in more recent reports by consumer and privacy advocacy organisations.[7]

In the European Union, the Article 29 Working Party[8] published an *Opinion on the Internet of things*.[9] The Opinion identified into six particular challenges:

(a) **lack of control and information asymmetry**: where device connectedness results in personal data generation, storage and communication over which the user has no control.

(b) **quality of user consent**: the user's consent to processing (collection and uses) of data carried out by IoT devices may not be fully informed. The affected individual may not even be aware of the relevant processing.

(c) **secondary use and repurposing**: data analysis techniques may lead to device data obtained for one purpose being used for a quite different purpose for which no consent has been given.

(d) **aggregation of data from different devices**: aggregation may reveal specific aspects of habits, behaviours and preferences of individuals in an unduly intrusive manner.

(e) limitations on the **possibility to remain anonymous** when using services.

(f) **security risks**: physical or cost constraints, including designing in battery efficiencies by compromising device security (confidentiality, integrity and availability).

This list is relevant, but incomplete.

---

[7] See for example Coll, L. & Simpson, R. (Consumers International, April 2016), "The Internet of Things and challenges for consumer protection", available at ; Australian Communications Consumer Action Network (ACCAN) (2017) "Security and privacy threats for smart-home IoT devices", available at https://accan.org.au/hot-issues/1449-how-safe-are-iot-devices; Rosner, G. & Kenneally, J.D. (The Internet of Things Privacy Forum) (May 2018) "Clearly Opaque: Privacy Risks of the Internet of Things", available at https://www.iotprivacyforum.org/clearlyopaque/; Which? (June 2018) "Control, Alt or Delete? The Future of Consumer Data", available at https://www.which.co.uk/policy/digitisation/2659/control-alt-or-delete-the-future-of-consumer-data-main-report. Examples of sector specific reviews include Mittelstadt, B. "Designing the Health Related Internet of Tings: Ethical Principles and Guidelines" ; Gray, S. (Future of Privacy Forum, April 2016) "Always On: Privacy Implications of Microphone-Enabled Devices" at https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf and similar materials available at https://fpf.org/best-practices/. See also Mathews-Hunt, K., (September 2017)"consumeR-IOT: where every thing collides: Promoting consumer internet of things protection in Australia", Unpublished PhD Thesis, Bond University, available at https://epublications.bond.edu.au/cgi/viewcontent.cgi?article=1228&context=theses. The U.S. National Institute of Standards and Technology recently released, and then withdrew, a "Draft Internal Report (NISTIR) 8222, Internet of Things (IoT) Trust Concerns", which identified seventeen technical trust-related issues that may negatively impact the adoption of IoT products and services. The document offered recommendations for mitigating or reducing the effects of these concerns while also suggesting additional areas of research with regard to the subject of "IoT trust". The note posted by NIST on withdrawal was "Draft NISTIR 8222 has been temporarily withdrawn to synchronize with other pending documents on this topic, and to ensure time for stakeholders to review and comment": https://www.nist.gov/news-events/news/2018/09/nist-releases-draft-nist-internal-report-nistir-8222-internet-things-iot.

[8] The Article 29 Working Party was an independent advisory body on data protection and privacy that was set up under the former data protection Directive 95/46. The successor organisation under the General Data Protection Regulation, the European Data Protection Board, has generally adopted such Onions and is likely to progressively adapt and revise them to address new and additional requirements of the GDPR.

[9] Article 29 Data Protection Working Party, "Opinion 8/2014 on 'Recent Developments on the Internet of Things" (14/EN WP 223, adopted as of 16 September 2014 (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf). See also U.S. Federal Trade Commission (June 19, 2018) "FTC Offers Comment on Process Aimed at Improving Security of Internet of Things Devices" https://www.ftc.gov/news-events/press-releases/2017/06/ftc-offers-comment-process-aimed-improving-security-internet); FTC Staff Report (January 2015) "Internet of Things – Privacy and Security in a Connected World", available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; NIST (November 2016) "Special Publication 800-160 - Systems Security Engineering – Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems", http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf, Privacy Commissioner of Canada (February 2016), "The Internet of Things: An introduction to privacy issues with a focus on the retail and home environments" https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/.

3.2 Multiple parties and separation of parties

(a) On the consumer side, often IoT services will be purchased by consumers separately from IoT platform and IoT sensor devices, and then set-up by consumers with those devices and smartphones and other control, reporting or actuation devices. Consumers may not fully understand how to manage risks through appropriate data and security settings. This characteristic creates potential demand side vulnerabilities that need to be managed through a consumer making appropriate data and security settings (if these capabilities have been made available by the IoT provider through in-designing of such capabilities). This in turn will often require building of understanding of consumers – and capabilities of consumers - about how to address these vulnerabilities.

(b) Often third party supplied devices will be integral to the service delivery chain. For example, a smart home applications may communicate with service providers by means of the Nest platform as bought and installed by the consumer and with the householder by an app on the householder's smartphone or tablet. The variety of device and service options may lead to issues as to responsibility for malfunction in provision of a service caused by failure of third party supplied devices or communications platforms and carriage services.

(c) IoT services often will be implemented into homes or other shared use environments where the activity monitored or reported on using an IoT device is an activity of a person (an 'affected individual') who is other than the consumer purchasing the IoT device or IoT service. This leads to concerns as to whether affected individuals will know about collection and use of information about their activities.

For example, many emerging B2C services are designed for in-home care of elderly or infirm users where the supported user is the affected individual and a remote carer or monitoring centre is provided with capabilities to configure, re-configure and control the IoT device. By their nature, these services requires sharing of sensitive personal information, not infrequently about an (identifiable) individual that may have limited capabilities to themselves understand or control uses of data about themselves. There is clear benefit to those individuals derived in personal dignity and enjoyment of life by staying in their homes. There is also social benefit through stable and supportive communities and reduction in costs of hospitalisation and crisis care. These benefits must be balanced against privacy impacts, while ensuring that privacy of these individuals is not jettisoned because they are disadvantaged by age, infirmity or other disability.

Further, estranged partners may be either protected from threatening ex-partners through good deployment of IoT services such as home monitoring, or vulnerable through inadvertent sharing with their threatening ex-partner of information derived from smart home IoT devices. Benefits, and dangers, will often be highly context specific: IoT services, like many data-driven services, can be tools for social and individual benefit, or tools for bad actors. The outcome is affected by both supply-side and demand-side factors. The delivered outcome will often depend upon the knowledge of consumers in setting up and monitoring their IoT deployments and the care that they take in so doing, as well as supply-side features in robustness, capabilities, transparency and intelligibility of designed-in privacy, security, interoperability and accessibility.

(d) Many IoT devices and IoT services are provided at very low price points and accordingly with inherent limitations as to robustness and capabilities of in-designed privacy and security that is commercially practicable at these price points.

A balance is required between:

- regulation that forces up the price points for IoT services to enable privacy and security for the 'haves' while leaving the 'have-nots' without the benefits of IoT services, and

- under-regulation that leaves a socially unacceptable level of vulnerabilities of cheaper IoT services and IoT devices to intrusions by (in particular) hacking or misuse of personal and otherwise sensitive information about individuals by bad actors.

(e) On the provider side, data will often pass through multiple parties (e.g. the service provider and its sub-contractors such as cloud platform service providers, data warehouses and billing service providers) working together in a data ecosystem to provide the full features and functionality of a service. Consumers are rightly concerned about collection and uses of personal information about them. However, their concerns do not begin and end with data privacy. IoT applications require trust between consumers and other affected individuals as to proper and sensitive handling of information about them by IoT service providers and all other entities involved in the IoT service delivery chain that have access to information about those individuals, including personal information. Providers should address vulnerabilities in IoT service end-to-end, including in operations of IoT data partners and including as to business confidential information, privacy and information security. These vulnerabilities need to be addressed through good practice measures including good data privacy and security by design, minimisation of data flows (and particularly data about individuals that are identifiable) within IoT services and IoT devices, and transparency as to collections, uses and disclosures of consumer data.

3.3 Reach

Many B2C IoT services reach into homes and other domestic, sometimes intimate environments, and enable observations and inferences as to private behaviour that otherwise are not possible.

Even where collected data may not be demonstrably about an identifiable individual (and therefore its use and collection regulated by privacy law), there will be reasonable expectations of some consumers as to full and fair disclosure as to collection and uses of consumer data collected in homes and other domestic environments, about children and disadvantaged (albeit non-identifiable) individuals.

3.4 IoT security concerns

Standards, protocols and protections as to IoT device security are still developing.

In this early stage of rollout of IoT services and development of security standards, poor security by design, poor implementation, or poor coordination or misunderstanding as to respective responsibilities of provider and user, may lead to unacceptable security vulnerabilities.

3.5 Undue reliance upon consumers to understand and mitigate risks

Consumers may place undue reliance upon reliability and availability of an IoT service. Consumers may not be aware of the extent to which reliability and availability of the service may be affected by factors outside the IoT service provider's control.

Conversely, an IoT service provider may assume that consumers will anticipate, monitor and mitigate particular risks, particularly through making appropriate security and privacy settings, updating software with security patches and ensuring that devices are appropriately located and monitored. However, consumers may not understand that these matters are their responsibility, or know how to assess and mitigate these risks.

3.6 Data quality

Data errors or omissions or breakdowns may also lead to incorrect decisions being made in reliance upon data analysis that is correctly carried out but using data that is adversely affected by data errors or outages. Because sensoring may rely upon proper operation of third party devices and some operating issues will not be capable of remote detection, the reliability of IoT services may be adversely affected by data quality issues of which the IoT service provider is unaware (even where the IoT service provider exercises all reasonable diligence in real-time monitoring of service quality).

3.7 Consumer Benefit

There is a significant prospect that concerns as to loss of control of data (for instance, that data may be used by competitors or others adversely to the interests of a data source or data controller), or as to information security of data as that data passes through the IoT service delivery chain, may significantly impede data sharing and provision of open IoT platforms and devices.

Unless these concerns are adequately addressed, a likely outcome will be to advantage fully integrated IoT service providers, closing out opportunities for specialist or niche providers. This would likely be adverse to innovative start-ups competing with vertically integrated global operators that can operate 'closed system' IoT services and therefore do not need to address the diverse issues associated with data sharing within an IoT service delivery chain. In other words, effective and predictable legal protection that facilitates data sharing within the IoT service delivery chain is likely to be more important to innovative start-ups than to vertically integrated global operators that provide 'closed system' IoT services, particularly where those operators conduct business from lightly privacy regulated jurisdictions.

3.8 Looking forward

We don't need to stoke fears of the unfamiliar: there are plenty of ill-informed commentators doing that already. But we do need to ensure that we don't become too familiar with the phalanx of IoT devices and services before we size them up. As humans affected by those devices, we are entitled to be told why we should consider that these devices reliably behave like responsible guests should we (or our employers) elect to invite them into our homes and workplaces. Our expectations of the behaviour of these guests are then informed by that conversation.

If our invitee IoT device/service walks, talks and looks like a duck, it should not be a piranha. We might then reasonably expect that our IoT device/service (Dr Henry Jekyll) should not transmogrify into evil Edward Hyde through remote software upgrade or changes to service

features and interconnectivity. Our family, housemates, other invitees or tenants should be able to reasonably expect that if they now cohabitate with Mr Hyde, they have been informed both that Mr Hyde is present and that he/she/it is Mr Hyde, not Dr Jekyll. If a service provider by remote software upgrade or change to service features or connectivity could transmogrify Dr Jekyll, we should of course know this – regardless of whether there is technically any handling of personal information involved. And if there is a substantial risk that Dr Jekyll could become Mr Hyde if we fallible consumers are careless but not manifestly stupid and allow Dr Jekyll to communicate with some nasty gang of irresponsible service providers, a service provider should tell us that. We can't expect to a service provider to address all of our manifest shortcomings and stupidities: the economy would stop if this was the law. However, it is not good enough to say that we are on our own and that we need to be especially intelligent in order to understand and control our smart invitees.

In the writer's view, consumers will likely soon demand greater transparency than has been expected of businesses to date as to diverse uses of data, for example, as to the pricing of services as offered to different customer segments or classes of users, or as to disclosures to law enforcement agencies or private litigants.

And while IoT services are becoming more complex and diverse, product lifecycles shortening and the number and range of participants in the IoT service delivery ecosystem increasing, businesses and consumers are demanding simpler forms of contract and more readily understandable operation and enforcement of consumer protection laws.

IoT businesses also need predictable operation of intellectual property laws and competition regulation, and availability of suitable radiocommunications spectrum (ideally, in the same spectrum bands in multiple markets) for low powered devices.

Autonomous capabilities of smart devices create particular concerns. We need to consider the appropriate, ethical and socially responsible limits to creation and deployment of autonomous capabilities in smart devices, and how to give effect to these limits in law and limitations as to freedom to contract out of those limits. In particular, we need to consider whether and when it is reasonable and fair for a supplier to shift responsibility to a buyer to determine whether and when to inform others about deployment and the use of a device and of the device's capabilities and limitations.

We now expect that user privacy and security should be by design and default. However, we don't yet expect that a product or service supplier should build accountability and accessibility by design into their offering, and should ensure that there is adequate transparency about who is told and who will know what a device is doing and how to control what the device does.

Nor does our law yet expect that there will be reasonable clarity as to who is responsible for what.

And the supplier often faces a dilemma: in a post-iPhone world consumers expect sleek and simple user interfaces and single page graphics driven deployment instructions. The required booklet of mandatory electrical warnings and warranty limitations is often consigned straight to the paper bin. More fulsome disclosures and instructions might well suffer a similar fate. But we do need to create a culture of better disclosure by suppliers, including as to their expectations of the level of responsibility to be exercised by consumers in relation to deployment and use of these devices. In short, we should apply to providers of smart devices and smart services the same expectations that, post Cambridge Analytica and

GDPR, we are now seeing develop about service providers informing and empowering users of online search and social networking services.

4 IoT Alliance Australia's *Good Data Practice Guide*

There are many initiatives underway in Australia, and in comparable jurisdictions, to formulate principles, guidelines or industry codes as to good industry practice in provision of various types of data driven services. These initiatives include proposed industry self-regulated schemes for business applications of data analytics and various industry sector or application specific initiatives.

The IoTAA's *Good Data Practice Guide* is intended to promote industry and consumer awareness as to good industry practice for provision of business to consumer (B2C) IoT services. The IoTAA suggests that an appropriate precautionary strategy is to promote consumer and industry awareness as to good industry practice for B2C IoT service implementation, to 'head off' problems and issues before they occur. The Guide focusses upon measures that IoT providers can take to build trust and understanding of consumers about safe use of IoT products and services. Recommendations include that providers ensure that terms of use of their products and services, and other communications with consumers, are fair and clearly expressed, particularly as to uses of consumer data and secure use of IoT devices.

This Guide does not focus upon particular IoT applications, instead taking a more general, economy-wide, approach. There have been very useful recent initiatives in some comparable jurisdictions addressing IoT related services as diverse as agricultural IoT services, telematic car insurance policies, IoT services involving recording of human speech, and so on. The IoTAA suggests that the principles for good information handling practices set out in the Guide are of general application in relation to IoT services and IoT devices regardless of industry sector or particular IoT application.

The Guide is drafted principally for use by providers of IoT B2C services and IoT consumer devices. The aim to assist providers in design of IoT services and provision of easily understood guidance about their safe use. It is also intended that the Guide will also assist development by IoTAA and consumer organisations of information materials for consumer about safe use of IoT services and devices.

The Guide was developed following extensive consultations with interested parties, including consumer organisations and regulators.

Conclusion

Industry initiatives such as the IoTAA Guide are required to anticipate and address concerns in relation to IoT services that otherwise may lead to reluctance by consumers to take-up IoT service, or possible regulatory or consumer backlash following reports of incidents arising due to poor practice in implementations of IoT services.

Providers and consumers have a mutual interest in anticipating and addressing possible concerns. Adverse effects caused by poor implementation of IoT services are likely to be suffered by many IoT service providers regardless of whether the root cause of a poor practice in implementation was an act or omission of the service providers suffering that adverse effect, or consumers not doing what they were expected to do.

In addition, industry players need to ensure that in deriving value from uses of customer data, they do so in a manner which demonstrates transparency, integrity and security, which facilitates customer trust and engagement in the IoT eco-system.

In short, industry and consumers need a better engagement model in order to ensure that IoT services deliver benefits without attendant consumer detriments. Industry can take positive steps to build that engagement model, but only by working with consumers and openly and frankly addressing their legitimate concerns.

Peter G Leonard
Principal, Data Synergies
Professor of Practice, UNSW Business School
Consultant, Gilbert + Tobin Lawyers

pleonard@datasynergies.com.au

5 October 2018