Horizon Scanning Series

The Internet of Things

Privacy, security and the Internet of Things

This input paper was prepared by Tony Joyner, Natasha Blycha, Alex Cook with contributions from Ariane Garside, Michael Faithfull, Oli Tod and Rafael Lawrence

Suggested Citation

Joyner, T, Blycha, N, Cook, A, Garside, A, Faithfull, M, Tod, O and Lawrence, R. (2019). Privacy, security and the Internet of Things. Input paper for the Horizon Scanning Project "The Internet of Things" on behalf of the Australian Council of Learned Academies, www.acola.org.

1 Introduction

The Internet Of Things (or "IoT") promises utility yet demands ubiquity.

For data to provide an insight, trigger an action, or unleash some new efficiency, it must be collected to begin with.[1]

The economic and technical incentives built into the IoT have led to IoT devices becoming ubiquitous throughout society. More data means greater insight, leading in turn (at least in theory) to improved efficiency, more desirable products and services, and greater financial performance.[2] There are now more IoT devices on earth than humans and the IoT is only increasing in size.[3]

However, just as the IoT gives rise to the possibility of significant economic return, it raises significant concerns relating to privacy, security and human rights. These concerns are not new. Since at least 1999, when the phrase "Internet of Things" was first used,[4] or perhaps since 1990, when the "Internet Toaster" first made its debut,[5] questions concerning the legal and ethical status of internet enabled devices have been raised.

Unfortunately, while answers to many of the technical challenges relating to the IoT have been forthcoming, progress in addressing the legal and ethical questions raised by the IoT is not keeping pace.[6] These legal and ethical questions do not neatly separate into clear categories. For example, security and privacy are deeply intertwined, and human rights considerations are a foundational base upon which most other concerns rest. They "intersect with each other in all sorts of ways, ranging from the simple to the complicated."[7]

Whether the IoT is deployed in a consumer or business context will significantly change the relevant considerations. In business contexts, many of the risks associated with the IoT can be successfully mitigated by prudent contract drafting and project management. For example, a well drafted smart legal contract, which can tie machine-executable code and IoT device data directly to contractual rights and obligations, can mitigate risk and assist in establishing consent. In consumer contexts, the often significant disparity in power between the supplier and the customer means that a forensic analysis of the privacy and security considerations is required, and a lower threshold for regulatory intervention will usually apply.

The IoT is also just one part of a broader trend of innovation, and considerations relating to other emerging technologies such as artificial intelligence, big data, and automation, should be imputed into any analysis of the IoT.

With these disclaimers in mind, we set out our views on the privacy, security and human rights implications of the IoT in this paper as follows. *First*, we consider the IoT's impact on privacy, focusing in particular on the impracticality of obtaining informed consent and

[1] Marco Iansiti and Karim Lakhani, 'Digital Ubiquity: How Connections, Sensors and Data are Revolutionizing Business' *Harvard Business Review* (November 2014) <https://hbr.org/2014/11/digital-ubiquity-how-connections-sensors-and-data-are-revolutionizing-business>.

[2] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (June 2015) <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.

[3] Mark Hung, 'Leading the IoT: Gartner Insights on How to Lead in a Connected World' *Gartner* (2017) <https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf>.

[4] Kevin Ashton, *That 'Internet of Things' Thing* (22 June 2009) <https://www.rfidjournal.com/articles/view?4986>.

[5] Robert Zakon, *Hobbes' Internet Timeline* (November 1997) <https://tools.ietf.org/html/rfc2235>.

[6] Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational ethical issues' (2018) 1-2 *Internet of Things Journal* 55, 55.

[7] Ibid, 56.

the limits on using the de-identification of data as a response to privacy concerns. *Second*, we set out a number of security concerns relating to IoT and suggest that any workable solution will include both technical and legal components. *Third,* we explore the issue of liability, outlining potential legal actions and defences that may be borne out of the IoT in both civil and criminal contexts. *Finally*, we consider discrete rights-based issues associated with IoT, namely those relating to workplaces, access and the use of IoT devices by children and other vulnerable groups.

When new technologies are adopted there is often a tension between short-term economic return and long-term legal and ethical considerations. The IoT is no different. While it represents a significant opportunity for improving the prosperity of all Australians, the IoT must be deployed carefully, with the risks relating to privacy, security, and human rights firmly front of mind.

2 Privacy

Privacy is a universal human right.[8] As set out in the Universal Declaration of Human Rights, "no one shall be subjected to arbitrary interference with [their] privacy, family, home or correspondence."[9] Despite this, it is often tempting to compromise or otherwise de-prioritise it in the name of technical innovation or economic progress. In the context of consumer IoT devices, any actual or potential infringement of an individual's privacy should be carefully assessed, and only accepted where there is a defensible rationale for doing so.

Concerning episodes relating to the privacy, or lack thereof, of consumer IoT devices have been reported. For example, smart home IoT devices have audibly laughed without user input,[10] and internet-connected televisions have recorded private conversations without first obtaining consent.[11] The sexual preferences and proclivities of IoT-enabled sex toy users have even been communicated over the internet.[12] The degree to which privacy considerations are relevant to IoT devices will be heavily dependent on context. For example, an IoT-enabled sex-toy will likely have greater associated privacy risks then an IoT-enabled kitchen appliance or light bulb.[13] The IoT has been described as a privacy "disaster waiting to happen,"[14] and privacy concerns are the most common reason why consumers do not purchase IoT devices for their homes.[15]

[8] Article 12, *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[9] Ibid.

[10] ABC News, '"I thought a kid was laughing behind me": Amazon's Alexa has been caught randomly cackling at people' *ABC News* (8 March 2018) <https://www.abc.net.au/news/2018-03-08/amazon-to-fix-alexa-laugh/9527412>.

[11] Chris Matyszczyk, 'Samsung's warning: our Smart TVs record your living room chatter' *CNET* (8 February 2015) <https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/>.

[12] We raise this as just one example of an extremely private, consumer-facing application of the IoT, where privacy and security considerations will be of particular importance. See Molly Redden, 'Tech company accused of collecting details of how customers use sex toys' *The Guardian* (15 September 2019) <https://www.theguardian.com/us-news/2016/sep/14/wevibe-sex-toy-data-collection-chicago-lawsuit>; Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational ethical issues' (2018) 1-2 *Internet of Things Journal* 55, 57.

[13] Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational ethical issues' (2018) 1-2 *Internet of Things Journal* 55, 57.

[14] Iliana Magra, 'Alexa Now Gives U.K. Users N.H.S. Medical Advice' *New York Times (*10 July 2019) <https://www.nytimes.com/2019/07/10/world/europe/alexa-nhs-amazon-privacy.html>.

[15] PwC, 'Preparing for the voice revolution' *PwC* (2019) <https://www.pwc.com/cisvoiceassistants>.

In Australia, the *Privacy Act 1988* (Cth) provides a regulatory framework for the collection of personal information through the Australian Privacy Principles.[16] The Australian Privacy Principles are designed to be technology neutral and able to adapt to emerging technologies.[17] However, the complexity of the IoT, particularly as it relates to other emerging technologies such as artificial intelligence and the increasingly globalised nature of data collection activities, as well as improvements in "re-identifying" otherwise de-identified data, raise a number of privacy concerns regarding the IoT which the current regulatory framework may not be able to address.

2.1 Informed consent

Data collection activities may be permitted where those whose data is being collected provide informed consent. However, it is difficult for the average person to comprehend, let alone consent to, the data collection activities of most IoT devices.

IoT devices are often new, often complex, and are increasingly being used in ways that are difficult even for technical users to comprehend. While most users comprehend on some level that their data is being collected, many do not sufficiently understand the degree to which their data is being collected, and the ways in which the data is being used.[18]

This causes significant difficulty, particular given the importance placed on obtaining informed consent in the Australian privacy regulatory framework. Consent may be express or implied and in either case must be obtained voluntarily.[19] This means that consent must be obtained in circumstances where the relevant individual is both adequately informed before giving consent, and has the capacity to understand and communicate their consent.[20] There has been significant research into how informed consent can best be obtained.[21] However, there is no easy answer.

In our age of ever-increasing technical complexity, the burden placed on those whose data is collected to properly review, understand, and consent to the personal information collection activities of IoT devices is significant and increasing by the day. This burden is compounded by the reality that the promised utility of IoT devices – productivity, insight and automation – cannot be obtained without at least some personal information or other data being collected. However, even where the benefits unlocked by the use of IoT devices are significant and accrue directly to those whose personal information is being collected, consent should not be assumed.[22]

Opt-out approaches to obtaining consent, whereby consent is assumed unless it is clearly withdrawn, are particularly concerning where IoT devices are passively collecting data. While opt-out approaches are not prohibited under Australian law, it is difficult to establish

[16] The Australian Privacy Principles are set out in Schedule 1 of the *Privacy Act 1988* (Cth).

[17] Office of the Australian Information Commissioner, *Australian Privacy Principles* (2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles/>.

[18] Fritz Allhoff and Adam Henschke, The Internet of Things: Foundational ethical issues (2018) 1 *Internet of Things* 55, 57-58.

[19] s6(1) *Privacy Act 1988* (Cth).

[20] Office of the Australian Information Commissioner, *Chapter B: Key Concepts - Australian Privacy Principle Guidelines* (22 July 2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/>.

[21] See, for example, Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational ethical issues' (2018) 1-2 *Internet of Things Journal* 55.

[22] This view is similar to that expressed by the Office of the Australian Information Commissioner. See Office of the Australian Information Commissioner, *Chapter B: Key Concepts* (22 July 2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/> B.38.

that informed consent took place in many such implementations.[23] Opt-out approaches are particularly complex or infeasible where the act of opting out is not socially accepted. For example, despite the privacy concerns associated with IoT devices, "if you go into somebody's home and they have [an IoT device], it's not really socially acceptable to say 'I'm actually going to turn around because I don't want to be in a house with that.'"[24]

Similar concerns exist where IoT devices are deployed in public spaces. It is difficult to "opt-out" if IoT devices are everywhere. Some "smart city" trials, which rely heavily on the use of IoT devices do not include any "surveillance-free" zones at all.[25] Further, where IoT devices are deployed by private entities the level of public oversight may be diminished, and any consideration of the public interest may be de-prioritised in favour of commercial priorities. Ultimately, the growing complexity and pervasiveness of the IoT makes providing truly informed consent a difficult – if not unrealistic – endeavour.

2.2 Consent Fatigue

"Consent fatigue" is a significant concern when assessing the impact of the IoT. It refers to the condition whereby those subject to privacy policies and other contractual frameworks governing the collection of data are increasingly overwhelmed by the number of policies they must review and consent to, and are unable to comprehend and adequately consent to the data collection and processing activities that are taking place.

The current best practice approach to obtaining informed consent is to use a privacy policy. However, while privacy policies may be current best practice, there is an increasing recognition that they may not necessarily be well suited for the digital economy. They have been described as an "incomprehensible disaster",[26] and have been criticised for being either overly technical or legal in nature (and therefore inaccessible to end users), or simply not detailed enough, "comprising of fairly generic boilerplate."[27]

Australian consumers feel "uninformed, unprotected and powerless" and 94% of Australian consumers have self-reported as not reading the privacy policies they are subject to.[28] Such behaviour has been described as "rational", on the basis that "it would take the average person 244 hours per year (6 working weeks) to read all privacy policies that apply to them."[29] The Australian Competition and Consumer Commission's recent review of the privacy policies of digital platforms found that each was between 2,500 and 4,500 words, and would take an average reader between 10 and 20 minutes to read.[30] Of those Australians who do read the privacy policies, two-thirds accepted terms with which

[23] Office of the Australian Information Commissioner, *Chapter B: Key Concepts* (22 July 2019) <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/> B.40.

[24] Madison Pauly, 'You Bought Smart Speakers Over the Holidays: Now What Are Amazon and Google Doing With Your Data?' *Mother Jones* (7 January 2019) <https://www.motherjones.com/politics/2019/01/amazon-echo-alexa-google-home-spying-on-me/>.

[25] See, for example, Ellen P Goodman and Julia Powles, 'Urbanism Under Google: Lessons from Sidewalk Toronto' (Draft) (2019) *Fordham Law Review,* Forthcoming <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3390610>.

[26] Kevin Ltman-Navarro, 'We read 150 privacy policies. They were an incomprehensible disaster' *New York Times* (12 June 2019) <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

[27] Fritz Allhoff and Adam Henschke, 'The Internet of Things: Foundational ethical issues' (2018) 1-2 *Internet of Things Journal* 55, 57.

[28] Consumer Policy Research Centre, *Research: Australian consumers 'soft targets' in Big Data economy* (13 May 2018) <https://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy>.

[29] Katharine Kemp, '94% of Australians do not read all privacy policies that apply to them – and that's rational behaviour' *The Conversation* (14 May 2018) <https://theconversation.com/94-of-australians-do-not-read-all-privacy-policies-that-apply-to-them-and-thats-rational-behaviour-96353>.

[30] Australian Competition and Consumer Commission, 'Digital Platform Enquiry' (Preliminary Report, December 2018) 368.

they were uncomfortable.[31] Oncone participant in research conducted by the Consumer Policy Research Centre stated that when consenting to privacy policies "I just close my eyes and don't think about it."[32]

Privacy policies are a rational approach to obtaining informed consent in circumstances where each act of data collection is considered in isolation. In our current environment, however, where Australian consumers are interacting with more and more data-collecting IoT devices every day, it may be akin to asking those who interact with the IoT to drink from a fire hose.

2.3 De-identification of data

De-identification refers to the process of taking data that is linked to a specific individual and altering or amending it to make such identification no longer possible.[33] Where informed consent cannot authentically be obtained, the de-identification of any data collected by IoT devices is both useful and pragmatic, yet insufficient.[34]

The increased prevalence of IoT devices is occurring in almost lockstep with an increased ability to re-identify data, and data that is considered as de-identified may not remain so for long.[35] While there have not yet been any claims of de-identified IoT device generated data being successfully re-identified in Australia, there are many examples of re-identification occurring more broadly.[36]

Information collected by IoT devices should be considered to be "dynamic", with its value, character and status as personal information or otherwise prone to change over time.[37] The risk of re-identification should be assessed contextually, with both the data and the environment in which it will be used considered.[38] The Office of the Australian Information Commissioner and the Commonwealth Scientific and Industrial Research Organisation have released a comprehensive framework to assist IoT device providers and users with adopting appropriate de-identification measures.[39]

Once a data set has been created and released it cannot be strengthened, only weakened by the future release of additional information that could assist re-identification efforts.[40] Further, even where de-identified data cannot be accurately re-identified, the

[31] Consumer Policy Research Centre, *Research: Australian consumers 'soft targets' in Big Data economy* (13 May 2018) <https://cprc.org.au/2018/05/13/research-australian-consumers-soft-targets-big-data-economy>.

[32] Ibid.

[33] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (21 March 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/>.

[34] This position is consistent with the approach taken by the Australian privacy regulator in relation to de-identification more generally. See Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (21 March 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/#ftn12>.

[35] See, for example, Luc Rocher, Julien Hendrickx and Yves-Alexndre de Montjoye, 'Estimating the success of re-identifications in incomplete datasets using generative models' (2019) *Nature Communications* 3069.

[36] See, for example, Paris Cowan, 'Health pulls Medicare dataset after breach of doctor details' *IT News* (29 September 2016) <https://www.itnews.com.au/news/health-pulls-medicare-dataset-after-breach-of-doctor-details-438463>.

[37] Office of the Australian Information Commissioner, *Guide to Data Analytics and the Australian Privacy Principles* (2019) <ttps://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/>.

[38] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (21 March 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/>.

[39] Christine M O'Keefe, Stephanie Otorepec, Mark Elliot, Elaine Mackey, and Kieron O'Hara, *The De-Identification Decision-Making Framework* (CSIRO Reports EP173122 and EP175702, 2017) <https://www.data61.csiro.au/en/Our-Work/Safety-and-Security/Privacy-Preservation/De-identification-Decision-Making-Framework>.

[40] Boris Lubarsky, 'Re-Identification of "Anonymised" Data' (2017) 1 *Georgetown Law Technology Review* 202, 202.

mere perception or possibility that it can be re-identified may lead to erroneous yet still damaging conclusions being drawn.[41]

Loss may occur even where there may not be a breach of the Privacy Act or other Australian regulation, and ethical and social considerations – not just legal obligations - should be taken into account by any entity.[42] This position is already endorsed by the Australian privacy regulator, the Office of the Australian Information Commissioner, and arguably should extend to all privacy considerations relating to the IoT - not just de-identification.[43]

2.4 Solutions

Privacy concerns relating to the use of IoT devices should be considered as part of the broader privacy concerns around the use of big data and artificial intelligence.

It is unlikely that a solution to the privacy concerns specific to the IoT will be found without also addressing the privacy concerns arising from these related other emerging technologies. Since the City of Perth deployment of Australia's first open-street closed circuit television (CCTV) system in July 1991, there has been significant policy debate justifying the use of surveillance and data collecting equipment in public spaces in Australia.[44] However, CCTV deployments have traditionally been justified on the basis of enhancing public security, whereas current IoT deployments have largely been motivated by economic interests such as a desire for greater operational efficiency or commercial insight.

The extent to which privacy should be traded off for economic gain should be closely examined. In a business context, where personal information is not being dealt with, this trade off can often be made on the basis of commercial interests only. The risk of possibly weakening the confidentiality of corporate information can be assessed against the value that an IoT deployments would likely provide. In consumer contexts, the burden of conducting such an assessment likely should not be put on each individual consumer. When the privacy of a consumer's personal information is at risk, a broader, regulation-based assessment should be undertaken.

IoT deployments should require a "privacy by design" approach, meaning that privacy is built into the design process and system architecture wherever possible.[45] Additionally, data minimisation should be embraced, with data – particularly personal information – only collected when there is a clear rationale for doing so.[46] Compliance with the principle of data minimisation is mandatory in the European Union, as it has been incorporated in the General Data Protection Regulations (GDPR).[47] The adoption of IoT devices in new fields such as healthcare will also bring new privacy considerations to the fore.

[41] Office of the Australian Information Commissioner, *De-identification and the Privacy Act* (21 March 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-and-the-privacy-act/>.

[42] Ibid.

[43] Ibid.

[44] Dean Wilson and Adam Sutton, 'Open-street CCTV in Australia' *Australian Institute of Criminology* (November 2003) <ttps://aic.gov.au/publications/tandi/tandi271>.

[45] Office of the Australian Information Commissioner, *Privacy by Design* (21 July 2019) <https://www.oaic.gov.au/privacy/privacy-for-organisations/privacy-by-design/>.

[46] Lydia de la Torre, 'What is "data minimization" under EU Data Protection Law?' *The American Bee* (23 January 2019) <https://medium.com/golden-data/what-is-data-minimization-under-eu-data-protection-law-b0e30fbb856e>.

[47] Article 5(1)(c) of the European Union General Data Protection Regulation – EU Regulation 2016/679.

As is typical of most technologies in their formative stages, the IoT market is highly fragmented.[48] There are many smaller players, who may not have the legal or regulatory sophistication of larger entities. A "move fast and break things" attitude may not be appropriate in circumstances where the IoT has the potential to impact on the right to privacy.[49]

3 Security

In both consumer and business-focused IoT devices, the security considerations are wide ranging.

The IoT enables insight, action, and automation all to occur at a distance. While the economic and productivity gains of these abilities are significant, cyber-based crimes - such as those enabled by the increasing ubiquity of IoT devices - have been described as the "ideal" attack vector for malicious actors.[50] To attack an environment through an IoT device placed within it, a malicious actor often does not need to bear the cost or risk of gaining physical access to the environment in order to cause it damage.[51]

Unfortunately, insufficient security in and around IoT deployments is common.[52] This has led some security experts to expand the "Internet of Things" moniker to the "Internet of Insecure Things",[53] and caused others to suggest that there are only two types of companies: those who have been hacked, and those who are simply not yet aware they have been hacked.[54] Views such as "pretty much all consumer internet of things vulnerabilities are avoidable" are frequently expressed.[55]

As IoT devices become ubiquitous, and as the data they collect increasingly automate actions of real consequence, the importance of securing the IoT will only increase. However, security can rarely – if ever – be obtained solely through technical innovation alone. The security of IoT devices is a multifaceted problem, and concerns relating to physical and infrastructure security, cybersecurity and operational security are all relevant. A co-ordinated, consistent and renewed focus on the security of IoT devices is required.

3.1 Physical and cyber security

Security issues are present in both discrete IoT devices and the infrastructure that connects them to each other and the Internet.

[48] Knud Lasse Lueth, 'IoT Investments 2018: $3.3B annual funding, record number of startup exits' *IoT Analytics* (3 October 2018) <https://iot-analytics.com/iot-investments-m-and-a-market-update-2018/>.

[49] Hemant Taneja, 'The Era of "Move Fast and Break Things" is Over' *Harvard Business Review* (22 January 2019) <https://hbr.org/2019/01/the-era-of-move-fast-and-break-things-is-over>.

[50] Ryan Jenkins, 'Cyberwarfare as Ideal War' in Fritz Allhoff, Adam Henschke and Bradley Jaw Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press, 2015) 89-114.

[51] Ibid.

[52] Juan Martinez, Jezreel Mejia, Mirna Munoz, 'Security analysis of the Internet of Things: A systematic literature review' (12 October 2016) *IEEE International Conference on Software Process Information.*

[53] Eliza Chapman and Tom Uren, 'The Internet of Insecure Things' *Australian Strategic Policy Institute* (19 May 2018) <https://www.aspi.org.au/report/InternetOfInsecureThings>.

[54] Nicole Perlroth, 'The Year in Hacking, by the Numbers' *New York Times* (22 April 2019) <https://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/ Nicole Perlroth>.

[55] Paul Roberts, 'Pretty Much All Consumer Internet of Things Vulnerabilities Are Avoidable' *The Security Ledger* (13 September 2016) <https://securityledger.com/2016/09/pretty-much-all-consumer-internet-of-things-vulnerabilities-are-avoidable/>.

IoT devices usually contain an embedded processor with onboard software and will often be connected through a number of intermediary connections, including cloud services, telecommunications networks, and local networks.[56] Security issues include hard-coded or difficult to change passwords or unclear or non-existent upgrade pathways.[57]

Where upgrade paths are impossible, or if an undue or otherwise unrealistic burden is placed on the end user to upgrade the IoT device's software or security, IoT device manufacturers have to get it right first time.[58] This is in conflict with the increasingly dominant "agile" approach to software development that encourages a more forgiving process of iteration and continuous improvement.[59]

The prevalence of programming errors is concerning, and can be explained in part as a trade-off between security and cost. Not all software is error prone. To cite one extreme example, the software controlling space-shuttle launches was "as perfect as human beings have achieved", with just one error in 420,000 lines of code.[60] This was, however, written by one of the United States' "most expensive software organisations".[61] A trade-off is required, and the extent to which security should be prioritised over competing considerations will be determined by context.

In certain applications of IoT, such as medical devices, security may take precedence over all other considerations. The United States' Department of Homeland Security has warned that malicious actors can "inject, replay, modify and/or intercept" data from medical devices.[62] In some business applications, the cost of implementing security may outweigh the resulting benefit, particularly if the IoT device is employed in a peripheral, or non-critical aspect of the business' operations.However, in almost all consumer applications of IoT(i.e. those where personal information is collected) and in sensitive business applications of the technology, the need for a comprehensive approach to security should rightfully act as a handbrake on IoT deployments.

3.2 National security

The security vulnerabilities apparent in the IoT are giving rise to several national security concerns.

The complexity of modern hardware supply chains, the lack of significant domestic IoT manufacturing activity, and the cost advantages enjoyed by most overseas IoT device manufacturers have made Australian users heavily reliant on IoT devices that are at least in part manufactured or assembled offshore.

The extent to which Australian regulators are equipped to assess or oversee the physical security risks associated with such IoT devices is unclear, and the burden on Australian

[56] IBM Analytics, *IBM Point of View: Internet of Things Security* (April 2015) <https://www.ibm.com/downloads/cas/7DGG9VBO>.

[57] Danny Palmer, 'New IoT security rules: Stop using default passwords and allow software updates' *ZDNet* (7 March 2018) < https://www.zdnet.com/article/new-iot-security-rules-stop-using-default-passwords-and-allow-software-updates/>.

[58] Edmund Brumaghin, Ross Gibb, Warren Mercer, Matthew Molyett and Craig Williams, 'CCleanup: A Vast Number of Machines at Risk' *Talos Intelligence* (18 September 2017) <https://blog.talosintelligence.com/2017/09/avast-distributes-malware.html>.

[59] Anh Nguyen Duc, Pangkaj Paul, Ronald Jabangwe and Pekka Abrahamsson, 'Security Challenges in IoT Development: A Software Engineering Perspective' (May 2017, Paper presented at the XP2017 Security Workshops) <https://www.researchgate.net/publication/319132115_Security_challenges_in_IoT_development_a_software_engineering_perspective>

[60] Charles Fishman, 'They Write the Right Stuff' *Fast Company* (31 December 1996) <https://www.fastcompany.com/28121/they-write-right-stuff>.

[61] Ibid.

[62] Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, Medtronic Conexus Radio Frequency Telemetry Protocol (21 March 2019) https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

security personnel to vet such devices is increasing. Further, even where IoT devices are functioning as intended, misunderstandings around features or inadequate guidelines for their use can nonetheless give rise to security vulnerabilities.

Even where IoT devices are not faulty *per se*, they may nonetheless give rise to security issues if insufficient consideration goes into their deployment.

3.3 Solutions

The choice between mandatory (e.g. legislated) and voluntary (e.g. industry-driven) responses to concerns regarding the security of the IoT is complex. To the extent that new mandatory requirements are imposed on IoT devices in Australia, they must be carefully drafted, or the resulting security benefit may be outweighed by a reduction in investment and innovation.

4 Liability

The IoT raises new and complex issues of liability. Resolving them has been described as a "legal feeding frenzy".[63]

The complexity stems both from determining who, as a matter of policy, should bear any loss, and how, as a matter of evidence, the cause of any loss can be identified.

Determining where any loss should be borne is a complex question. For example, losses can be borne by:

- those who suffer the loss in each case (e.g. the users whose data is compromised, or the businesses whose operations are affected by malfunctioning IoT devices);
- the responsible entities in each case, assuming they can be identified (e.g. traditional civil liability, where the one who commits the act is responsible for its consequences);
- the broad category of people who are likely to suffer loss (e.g. a compensation scheme that is funded by the users of IoT devices);
- the broad category of people who are likely to cause such losses (e.g. a compensation scheme that is funded by a tax on the manufacture or supply of IoT devices);
- an industry body (e.g. a compensation scheme funded by an IoT association); or
- the state (e.g. a compensation scheme funded by the general treasury).[64]

Determining which of these options is desirable in the context of the IoT is a question that can often only be answered on a case-by-case basis, with reference to the specific social and moral context as is apparent on the available facts.

As a matter of evidence, it is often difficult to identify which entity involved in the IoT is to blame for any loss. The users, the manufacturers, the developers of embedded or enabling software, the vendors of the IoT devices or software, as well as the providers of any connecting telecommunications infrastructure are all stakeholders in any IoT

[63] Lindsey O'Donnell, 'Black Hat 2018: IoT Security Issues Will Lead to Legal "Feeding Frenzy"' *Threat Post* (13 August 2018) <https://threatpost.com/black-hat-2018-iot-security-issues-will-lead-to-legal-feeding-frenzy/134997/>.

[64] These options are adapted from those put forward by Guido Calabresi. See Guido Calabresi, *The Costs of Accidents* (Yale University Press, 1970) 22.

deployment, and any or all of them could contribute to a given loss. Identifying the separate contributions of each is often a convoluted process.[65]

Where the relevant counterparty can be identified, possible actions include claims in negligence, product safety defects, breaches of the privacy legislation, or breaches of contractual terms (such as the sale contract between an IoT device manufacturer and the end user). Depending on the action brought against them, a party (the defendant) may have none, one, or several defences available to them as against a plaintiff.

For example, for tort-based claims a user of an IoT device may have acted in a way that is contributorily negligent (such as by incorrectly configuring their devices), have otherwise failed to take reasonable care, or even assumed the risk of an obvious hazard.

For contractual claims, a defendant may rely on contractual protections such as indemnities and exclusion clauses or may have drafted their obligations in such a way that there is no breach to begin with. Defences of this nature may be limited under law, such as where they are considered to be unfair contract terms.[66]

For defective goods claims brought under the Australian Consumer Law, an action may be successfully defended by establishing that the state of scientific or technical knowledge at the time when the goods were supplied was not such to enable the relevant defect to be discovered.[67] This "start of the art" defence is rarely relied upon in Australia.[68] Notably, a "small statistical chance of injury" associated with a given product does not of itself mean that it is defective.[69] While most commentary on this defence is grounded in a pharmaceutical context,[70] it may prove of use in cases concerning the IoT. Simply because an IoT device gives rise to some inherent small and statistical chance of injury should not necessarily imply that it is defective. Such a risk may be accepted where the economic benefit is sufficiently high.

In any event, the impact of the IoT on questions of liability, and its treatment under the law, is complex and difficult to predict. In addition to its impact on civil claims, the extent to which the IoT is enabling new forms of domestic violence or other criminal activity is only just beginning to be understood.[71]

The increased prevalence of consumer IoT devices has been described as creating "a stalker's paradise", with malicious actors potentially enjoying greater visibility as to people's location, behaviour and habits through the analysis of IoT device data. [72] Internet

[65] Jeffrey Voas and Phillip Laplante, 'The IoT Blame Game' (2017) 50(6) *IEEE Computer* 69.

[66] See generally *Competition and Consumer Act 2010* (Cth) sch 2, ss 23 – 28.

[67] *Competition and Consumer Act 2010* (Cth) sch 2, s 142(c).

[68] There have been only two prominent cases dealing with the state of the art defence in Australia. See *Graham Barclay Oysters Pty Ltd v Ryan* [2000] FCA 109 and *Peterson* v *Merck Sharpe & Dohme (Australia) Pty Ltd* [2010] FCA 180. In both cases it was found that the state of the art defence was available to the defendant.

[69] Such a view has been found in the Explanatory Memorandum, Trade Practices Amendment Bill 1992 (Cth), 8 cited in Mabel Tsui, 'The State of the Art Defence: Defining the Australian Experience in the Context of Pharmaceuticals', (2013) 13(1) *QUT Law Review* 132, 133.

[70] Mabel Tsui, 'The State of the Art Defence: Defining the Australian Experience in the Context of Pharmaceuticals', (2013) 13(1) *QUT Law Review* 132.

[71] See, for example, Dr. Leonie Tanczer, Dr. Simon Parkin and Professor George Danezis, *The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT)* (2018) <https://www.ucl.ac.uk/research/domains/collaborative-social-science/social-science-plus/IOT-and-domestic-violence>.

[72] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart and Nicola Dell, ' "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology," (2018, Paper No. 667) *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

connected thermostats, locks and lights have all been used to enable or otherwise facilitate acts of violence.[73]

While new criminal actions could be proposed to deal with this emerging threat, this may not be required. Existing criminal act classifications, including but not limited to stalking, fraud, illegal surveillance, and possession of a surveillance device may already capture most instances of IoT devices being used for criminal purposes.[74]

Addressing the general privacy and security concerns outlined above will hopefully go some way to mitigating the risk of IoT devices being used to enable or commit crimes. The risk of the IoT enabling criminal activity should be carefully monitored and a legislative or policy response may be necessary in the future.

4.1 Evidentiary value of IoT Data

The emergence of IoT-generated data and insight will likely impact on the determination of liability.

The prudent use of IoT devices may be used to reduce the probability of a dispute occurring, or to more easily settle or determine claims when disputes do arise. While not yet common in Australia, the use of IoT device data as evidence is already occurring overseas.[75] The evidentiary and policy considerations relating to the use of IoT device generated data in legal proceedings are significant.

In both consumer and enterprise contexts, IoT devices are usually designed to passively collect data on an ongoing basis.[76] The extent to which this data can be requested by criminal law enforcement, or plaintiffs in civil proceedings, needs to be carefully managed. Records from IoT smart home devices have already been requested in international court proceedings.[77] “Fishing expeditions” - where IoT device data is requested solely on the basis that the IoT data may or may not have evidentiary value - will need to be carefully monitored.

Simply being aware that a criminal act or civil contravention occurred in a specific venue may or may not be of sufficient probative value for access to the data collected by nearby IoT devices to be granted. A case-by-case analysis will be required.

5 Other considerations

In the reminder of this paper we turn to address issues that the IoT raises in relation to the rights of specific groups, such as employees, children, and rural, regional and remote communities.

[73] Nellie Bowles, ‘Thermostats, Locks and Lights: Digital Tools of Domestic Abuse’ *New York Times* (23 June 2018) <nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html>.

[74] Domestic Violence Resource Centre Victoria, *Legal Guides (2019)* <https://www.dvrcv.org.au/knowledge-centre/legal-protection-safety/legal-guides/>.

[75] See, for example, Clifford Katz, Joe Meadows, Laura Aradi and Paul Mathis, ‘Recent IoT Device Cases’ *Crowell Moring* (10 July 2017) <https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/>.

[76] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (June 2015) <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.

[77] Digital Trends, ‘*New Hampshire judge tells Amazon to turn over Echo recordings in murder case*’ (2018) <https://www.digitaltrends.com/news/alexa-court-new-hampshire-judge-requests-echo-recordings/>.

5.1 Workplaces

Where IoT devices are used in the workplace, the possibility of significant gains in productivity and profitability are clear.[78] It has been suggested that the hype around the potential benefit of deploying IoT devices in workplaces "may actually understate the full potential."[79]

However, issues relating to the surveillance or control of worker activities, as well as broader questions around the displacement of work, arise.

The right to work includes both the rights to "free choice of employment, to just and favourable conditions of work and to protection against unemployment"[80] and the right "to form and join trade unions for the protection of [an employee's] interests."[81] The use of IoT devices in the workplace may challenge these rights, and pose questions relating to the extent to which an employer's legitimate interests in both operational efficiency and oversight over their workplace should be balanced against an employee's equally legitimate interests, including their right to privacy.

Confrontations between employees and employers over the use of IoT devices to analyse or monitor performance are becoming common. As just one example, Australia Post "categorically ruled out" the use of IoT devices to monitor its employees' performance after concerns were raised by the relevant union.[82] Australian courts are already being asked to consider the impact of IoT devices on workplace rights, including employee privacy.[83]

The degree to which Australian employees will be able to negotiate restrictions on the use of IoT devices in the workplace will vary significantly on a case-by-case basis, and regulatory guidance may be required to provide certainty as to the allowed limits on such IoT deployments.

5.2 Access

Similarly, regulatory action may be required to create minimum standards for the accessibility of IoT devices.

While there are clear standards for maximising the Internet's accessibility more generally, there are not specific standards for the IoT. Device makers have taken an adhoc and inconsistent approach to ensuring that IoT devices are accessible.[84] This lack of standardisation has likely been a barrier to increasing the accessibility of the IoT, as providers of IoT devices must customise their approach to accessibility for each specific application or device.

---

[78] McKinsey Global Institute, *The Internet of Things: Mapping the Value Beyond the Hype* (June 2015) <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world>.

[79] Ibid.

[80] Article 23(1), *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[81] Article 23(4) *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[82] Julian Bajkowski, 'Australia Post rules out video performance "monitoring" of staff amid union row' *IT News* (14 March 2019) <https://www.itnews.com.au/news/australia-post-rules-out-video-performance-monitoring-of-staff-amid-union-row-520522>.

[83] See, for example, *Jeremy Lee v Superior Wood Pty Ltd* [2019] FWCFB 2946, where the Full Bench of the Fair Work Commission was required to consider the lawfulness of an employer directing an employee to provide their biometric data via an IoT device.

[84] See, for example, 'Delivery of outcomes under the National Disability Strategy 2010-2020 to build inclusive and accessible communities (Senate, Community Affairs References Committee, November 2017) 41.

Additionally, the IoT, like most emerging technologies, is being deployed in an inconsistent manner. Households in rural, remote and regional communities are twice as likely to not have an internet connection as those in metropolitan areas.[85] While this is explainable due to the higher cost of deploying infrastructure to such locations, it nonetheless has the potential to create a "a substantial digital divide."[86]

Making the provision of public or otherwise crucial services contingent on access to or possession of some form of IoT device, may aggravate the difficulties that individuals in such environments already have with obtaining access to such services.

5.3 Children

The security and privacy concerns associated with the IoT are magnified where IoT devices are used by children. Internet connected toys directly targeting at children are available,[87] and children have indirect access to other IoT devices, such as smart speakers, in the household. Breaches of children's privacy through the IoT have already occurred. For example, an "Internet of Things Teddy Bear" was found to have leaked over two million private audio recordings of parents and children due to misconfigured security settings.[88] One analysis of the Amazon "Echo Dot" smart speaker found that, of the features targeted explicitly at children, more than 80% were not covered by a privacy policy.[89] The study found that "even the most diligent parent" would not be able to ascertain what information the IoT device was collecting about their children.[90]

6 Conclusion

Like many other emerging technologies, the IoT promises a great deal yet asks much in return. Ensuring its security and privacy must be front of mind for all. In broad terms, the security and privacy of IoT devices and the data they create is of direct relevance to the maintenance of several human rights, including freedoms of privacy,[91] expression,[92] and association.[93] Protecting these rights, and addressing the security and privacy concerns inherent in the IoT should not be considered a barrier to progress. Such acts would lead to increased trust, which in turn would engender greater support for innovation and progress.[94]

[85] Australian Bureau of Statistics, *8146.0 - Household Use of Information Technology, 2016-7* (28 March 2018) <https://www.abs.gov.au/ausstats/abs@.nsf/mf/8146.0>.

[86] Roy Morgan, *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2018* (2018) <https://digitalinclusionindex.org.au/wp-content/uploads/2018/08/Australian-digital-inclusion-index-2018.pdf>.

[87] Marie-Helen Maras, '4 ways "internet of things" toys endanger children' *The Conversation* (10 May 2018) <https://theconversation.com/4-ways-internet-of-things-toys-endanger-children-94092>.

[88] Dan Goodin, 'Creepy IoT teddy bear leaks >2 million parents' and kids' voice messages' *Ars Technica* (28 February 2017) <https://arstechnica.com/information-technology/2017/02/creepy-iot-teddy-bear-leaks-2-million-parents-and-kids-voice-messages/>.

[89] Echo Kids Privacy, 'Kid Skills Privacy Analysis' (2019) <https://www.echokidsprivacy.com/>.

[90] Ibid.

[91] Article 12, *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[92] Article 19, *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[93] Article 20, *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948).

[94] This view has been endorsed by the Australian privacy regulator, the Office of the Australian Information Commissioner. See Office of the Australian Information Commissioner, *Guide to Data Analytics and the Australian Privacy Principles* (2019) <ttps://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/>.

Tony Joyner
Sector Lead Partner – Technology, Media and Telecommunications, Herbert Smith Freehills

Natasha Blycha
Global Head of Digital Law, Herbert Smith Freehills

Alex Cook
Graduate – Technology, Media and Telecommunications, Herbert Smith Freehills and Adjunct Lecturer, University of Western Australia Law School

10 September 2019

Note: Ariane Garside, Michael Faithfull, Oli Tod and Rafael Lawrence assisted in preparing this paper.