**INTERNET OF THINGS AND PRIVACY**

**ISSUES AND CHALLENGES**

**CONTENTS**

[INTRODUCTION 3](#_Toc69736525)

[PERSONAL INFORMATION 3](#_Toc69736526)

[RELATED TECHNOLOGIES 4](#_Toc69736527)

[Artificial intelligence 4](#_Toc69736528)

[Cloud computing 4](#_Toc69736529)

[Network technologies 5](#_Toc69736530)

[PRIVACY ISSUES 5](#_Toc69736531)

[Collection, use and disclosure of IoT data 5](#_Toc69736532)

[De-identification of IoT data 6](#_Toc69736533)

[Consent 7](#_Toc69736534)

[Dependency on vendors 8](#_Toc69736535)

[Interoperability 9](#_Toc69736536)

[Managing IoT devices 9](#_Toc69736537)

[Accountability 10](#_Toc69736538)

[Transparency 10](#_Toc69736539)

[CONCLUSION 11](#_Toc69736540)

INTRODUCTION

The Internet of Things (**IoT**) is a broad term that generally refers to physical devices connected to the internet that collect, share or use data. This includes personal wearable devices such as watches and glasses, home appliances such as televisions and toasters, features of buildings such as lifts and lights, supply chain and industrial machinery such as forklifts and sprinklers, and urban infrastructure such as traffic lights and rubbish bins.

IoT devices and the data they collect can provide convenience, efficiency and insights into essentially every aspect of our world. For the public sector, the IoT is currently providing many benefits and has the potential to generate even greater public value in the future.

Smart bins can alert waste trucks when they are nearly full, networked ticketing systems can help optimise public transportation, and automated attendance systems can free up time for teachers in classrooms.

Consumers, governments and businesses everywhere have been increasingly using IoT devices, and it is widely expected that the use of IoT will continue to expand rapidly. However, rushing into the IoT without proper consideration of privacy can lead to harmful and unexpected consequences. As the IoT grows, the amount of data it generates will naturally increase alongside it. These large collections of data can, in many cases, constitute personal, health and sensitive information, raising many privacy challenges.

This resource has been developed to assist the Victorian public sector in understanding some of these challenges. It may also be useful to a broader audience.

PERSONAL INFORMATION

It is very common for privacy laws, such as Victoria’s *Privacy and Data Protection Act 2014,* to focus on the protection of personal information. While the definition of personal information varies between jurisdictions, it normally refers to information about an identified or identifiable individual.

Privacy laws generally protect personal information by giving individuals control over how their personal information is handled by governments and businesses. Organisations using IoT devices that collect or use personal information must abide by laws and regulations that prescribe how personal information can be handled.

Wearable and home IoT devices frequently collect personal information, including biometric data such as voice and gait characteristics, and personal preferences such as eating habits and preferred TV shows. These devices, and the data they collect, can be used to provide great convenience and benefits to consumers. For example, smart climate control systems can be controlled remotely and fitness trackers can provide personalised workout routines to their wearers.

Outside of consumer IoT devices, the amount of personal information collected can vary greatly. Smart buildings can use smart heating and lighting systems to greatly reduce energy consumption without collecting personal information. On the other hand, a building could have an IoT reception system to automatically verify the identity of visitors and issue them an access card, requiring the collection of personal information.

Smart cities often collect massive amounts of data, however whether or not those data collections are personal in nature can vary from city to city. It is common for smart cities to use IoT devices to collect data about the movements of pedestrians, public transport riders and traffic, as well as information about water and electricity usage. Data such as this can provide detailed insights into how cities work and can lead to better informed decisions. However, if smart city data is personal information, such as movement data linked with identified individuals, it can be potentially invasive and carries a greater risk of being misused.

As the name suggests, the Industrial Internet of Things (**IIoT**) refers to the rapidly growing practice of using IoT devices for industrial applications. The industrial focus of IIoT ecosystems means that they generally collect less personal information than regular IoT ones. However, the IIoT is not without privacy issues. For example, trucks and other heavy vehicles can have IoT devices that identify when a driver is fatigued, alerting their employer; and factory workers can wear wristbands that sense when they are fidgeting or procrastinating for extended periods of time, potentially leading to disciplinary actions.

Much of the data collected by IoT devices, personal or otherwise, was previously difficult to collect. For example, some fitness trackers can measure blood pressure, something that otherwise requires specialised equipment to collect. With millions of fitness trackers, the blood pressure of large groups of people can easily be collected. Data such as this could benefit everyone through better health research, but it could also cause harm if used inappropriately, such as by an insurer raising the premiums of fitness tracker users with high blood pressure.

RELATED TECHNOLOGIES

The IoT contains and interacts with a broad range of technologies. This section will briefly cover the most relevant ones.

Artificial intelligence

Artificial intelligence (**AI**) is a field of computer science with the goal of creating computer systems that can perform tasks that normally require human intelligence. AI commonly performs tasks such as identifying objects, transcribing speech, making decisions and so on.

The most effective forms of AI at the moment are based on deep neural networks, which require large amounts of data to learn and work. The data collected by the IoT is well suited for use by AI, which in turn can provide IoT devices with functionality such as processing voice commands.

Cloud computing

The cloud refers to networks of computers that are used remotely instead of locally. It is made up of software, platforms and infrastructure that is provided on-demand to users. Common cloud services include running applications and storing, processing and delivering data.

IoT devices frequently use a range of cloud services. Data collected by IoT devices is often stored or processed on cloud platforms, primarily due to the scalability of cloud and limits on storage and processing power on small IoT devices, but also because many IoT companies see additional value in being able to easily access data from IoT devices.

Network technologies

IoT devices are almost always connected to the internet or private networks. Wearable, home and office devices tend to connect to networks using short range technologies such as Ethernet, Bluetooth or WiFi, while larger IoT ecosystems such as those in cities or farms often use longer range technologies such as cellular or satellite networks.

5G is a cellular network technology set to replace 4G. For the IoT, 5G will bring a range of benefits such as allowing many more devices to be simultaneously connected,[[1]](#endnote-1) and being able to track the location of those devices with considerably higher precision and accuracy.[[2]](#endnote-2)

PRIVACY ISSUES

As noted above, the IoT poses a number of challenges to information privacy. This section provides an overview of the kinds of privacy challenges organisations and individuals can face.

Collection, use and disclosure of IoT data

The data collected from IoT devices generally comes from sensors including microphones, accelerometers and thermometers. Data from sensors such as these is often highly detailed and precise. This granularity allows additional information to be easily created through machine learning inferences and other analysis techniques that can yield results that would not be possible with coarser data.[[3]](#endnote-3)

In addition, devices with multiple sensors, or multiple devices in close proximity, can combine their data in a process known as sensor fusion, which allows for more accurate and specific inferences that would not be possible with data from a single sensor.[[4]](#endnote-4) For example, sensor data about the temperature, humidity, light level and CO2 of a room can be combined to track its occupancy with considerably higher accuracy than would be possible with only one of those kinds of data.[[5]](#endnote-5)

Inferences such as these can be extremely useful for a range of purposes, but they can also be highly personal and unexpected. Individuals are generally uncomfortable with organisations using IoT data to infer information about them.[[6]](#endnote-6) For example, IoT devices such as smart speakers can use inferences to make sales pitches,[[7]](#endnote-7) however, the use of inferences in this way can pressure individuals into making transactional decisions that they otherwise would not have made,[[8]](#endnote-8) particularly if they take place in a non-retail environment such as a home.[[9]](#endnote-9)

Care should especially be given to the purposes for which data is used when it is collected from people who have no choice. For example, the energy efficiencies created by smart meters and the ease of servicing them can cause utility organisations to cease offering and supporting traditional energy meters,[[10]](#endnote-10) meaning that residents may have no choice but to use smart meters.

However, smart energy meters can reveal a range of profoundly personal information about individuals,[[11]](#endnote-11) including obvious information such as how often they use their washing machine, and less obvious information such as which television shows they watch.[[12]](#endnote-12) Organisations such as insurers, advertisers, employers, and law enforcement are likely to find data and inferences from IoT devices such as smart meters highly valuable.[[13]](#endnote-13) However, care must be given to the appropriateness of using and disclosing such data when opting-out is not possible.

When personal information is collected by public IoT ecosystems such as smart cities, consideration must be given to who will own and control the information, and for what purposes it will be used. When a public entity like a city partners with a private organisation to use IoT devices or services, the city must ensure that personal information will be used and disclosed in line with the best interests of the citizens of the city.[[14]](#endnote-14) If private organisations that provide IoT devices or services can access IoT data, there is a risk that they could use or disclose personal information for purposes that are not in the public interest, such as for profiling, targeted advertising or sale of the data to data brokers.

At a more abstract level, humans change their behaviour when they are aware that there is a possibility they are being watched, causing them to self-police and self-discipline.[[15]](#endnote-15) Online, users constrain and censor themselves based on who could potentially see their activities.[[16]](#endnote-16) And when smartphones first became ubiquitous, the ability to easily upload information caused a ‘chilling effect’, in which people modified their ‘offline’ behaviour in response to the possibility of what could be made available online.[[17]](#endnote-17) It is currently unclear what effects the IoT could have on human behaviour and freedoms of expression through widespread data collection; one possibility is that the ‘chilling effect’ could spread to previously private spaces such as homes.[[18]](#endnote-18)

IoT devices can also allow practices that were previously only possible online to occur in physical spaces. For example, retail stores can restrict entry to people who have created an account through the use of automated gates that require an app to pass through.[[19]](#endnote-19) Online, AI can be used to predict how much a customer would be willing to pay, allowing a store to adjust its prices accordingly.[[20]](#endnote-20) IoT devices could potentially allow brick and mortar stores to easily perform similar price targeting.[[21]](#endnote-21)

De-identification of IoT data

The data collected by large IoT ecosystems like smart cities can be valuable for a range of purposes such as research or informing policy decisions. A common way to maximise the value of this data is to make it publicly available online. However, it is generally impermissible for datasets that include personal information to be made publicly available.

The simplest way to ensure personal information is not included in a dataset is to allow individuals to remain anonymous by never collecting information that can identify them. For example, a smart city could count pedestrians using IoT sensors that record movements, instead of images or video.[[22]](#endnote-22)

The process of removing personal information from a dataset is called de-identification. However, data collected by the IoT is often very difficult to de-identify due to its highly granular nature.[[23]](#endnote-23) Longitudinal information is especially hard to de-identify,[[24]](#endnote-24) even when aggregated.[[25]](#endnote-25)

A common way that organisations attempt to remove personal information from data collected from IoT devices is through hashing, transforming the data by means of an algorithm.[[26]](#endnote-26) However, hashing does not permanently de-identify information; instead it pseudonymises information by replacing an identifiable individual with what is effectively a unique identifier. While hashing can be useful for protecting personal information in some cases, hashed information is generally very easy to re-identify.[[27]](#endnote-27)

There are many other risks with sharing non-personal or de-identified IoT data with third parties. For example, the receiving organisation could use auxiliary information to re-identify it;[[28]](#endnote-28) AI could infer personal,[[29]](#endnote-29) or even sensitive,[[30]](#endnote-30) information from the dataset; and if the dataset is used to train an AI model which is then shared, information about individuals in the dataset could be revealed.[[31]](#endnote-31)

Consent

Consent is a common basis for organisations to use and disclose personal information. However, valid consent generally requires more than getting a user to click ‘I agree’. Meaningful consent has five elements: capacity, voluntary, current, specific and informed. The IoT challenges each of these elements.

Capacity

An individual must be capable of giving consent for it to be valid. A common reason that an individual does not have the capacity to consent is because they are a minor. For IoT devices targeted to children, such as smart toys, or devices designed to monitor children, such as IoT tracking wristbands, an authorised representative such as a parent or guardian may consent on behalf of the child. However, whether or not a minor is capable of providing consent becomes less clear as they mature. For IoT devices aimed at parents who want to monitor their teenagers,[[32]](#endnote-32) consent can be complicated.

Voluntary

Consent must be freely given in order to be meaningful. It must be a genuine choice. If an individual must choose between giving consent or not being able to use a device they have purchased, then that consent may not be voluntary. If accepting terms and conditions is a prerequisite to using an IoT device and refusing those terms will result in an inoperable device, it is likely not a genuine choice and therefore not meaningful consent.

In addition, IoT devices in shared spaces like smart cities, retail stores, smart homes or connected cars generally do not have an opportunity to provide notice and obtain consent from every person whose information is collected.[[33]](#endnote-33) Even if a device does have an opportunity to provide information and collect consent, the consent may not be meaningful if individuals have to choose between consenting or not entering a physical area.

A similar situation occurs when employers require employees to wear IoT devices.[[34]](#endnote-34) The purpose of these devices is generally to collect information about employees. For example, IoT wristbands can monitor warehouse workers’ performance;[[35]](#endnote-35) smart badges can measure the tone of voice, excitement and passion of call centre staff;[[36]](#endnote-36) and chemical sensors placed on doctors can detect when they have gone too long without washing their hands.[[37]](#endnote-37) If using devices such as these is a condition of employment, it is likely not possible for an employee to provide voluntary consent to the use of information collected by such a device, as if they choose not to give their consent, they may be ineligible for the job.

Current

Consent cannot be assumed to last indefinitely. The seamless and unobtrusive nature of IoT devices often makes it easy for people to forget they are there or what they are doing. Smart devices such as watches, doorbells, and billboards can blend into the background as they collect, use and share personal information.

Additionally, the way that an IoT device operates can also change over time. For example, a device may have a sensor that is inactive and serves no purpose when the device is first brought to market, but the vendor may later enable the sensor and introduce features that utilise it.[[38]](#endnote-38) Alternatively, an IoT vendor could be acquired by a different company that has different privacy practices, or could collect and use personal information for new purposes that existing users may not expect.[[39]](#endnote-39)

One off ‘I agree’ consent mechanisms are a single decision at a single point in time that may be inappropriate for the ongoing and evolving nature of the IoT.

Specific

Consent must be specific to an identified purpose. It is not possible for an individual to provide meaningful consent to their personal information being used for a vague or broad purpose. If an IoT device provides unspecific information, users can develop misconceptions about what happens to personal information collected by the device and can be surprised when they discover what they actually agreed to.[[40]](#endnote-40)

Informed

An individual must have full knowledge of all relevant facts for their consent to be meaningful. This includes, but is not limited to:

* what information will be collected, used or disclosed;
* the purpose for collecting the information; and
* who the information will be shared with and what they will do with it.

The complex interactions between the functions of an IoT device – and the interactions between different devices, organisations and third parties – can make it difficult for users to develop mental models for visualising how their devices operate, what information they collect, and how they use and disclose that information.[[41]](#endnote-41) When users do develop mental models, they can be inaccurate due to being based on misplaced assumptions about how devices work.[[42]](#endnote-42) Users may be further confused by extensive IoT terminology and jargon that is often used inconsistently.[[43]](#endnote-43) In addition, AI inferences can make it hard for individuals to understand what organisations could learn about them from information collected by IoT devices.[[44]](#endnote-44)

These factors, compounded by transparency issues discussed later, can make it difficult for individuals to understand how an ecosystem of IoT devices, infrastructure and organisations work, which can ultimately make it difficult for individuals to provide informed consent.

Dependency on vendors

Organisations and individuals who use IoT devices are often dependant on the vendors or manufacturers of those devices to handle security and privacy issues through the delivery of software or firmware updates to fix security vulnerabilities. Sometimes they are reliant upon vendors to ensure that collected personal information is sufficiently de-identified before it is shared.

However, vendors often focus on specific parts of IoT ecosystems and will not necessarily consider how those ecosystems function holistically.[[45]](#endnote-45) Vendors may also be based in jurisdictions with less adequate privacy legislation. They also frequently prioritise ease of use, novel functionality, and getting to market quickly, over privacy and security risks.[[46]](#endnote-46) Consumer IoT device manufacturers are predominantly consumer goods companies rather than software or hardware companies.[[47]](#endnote-47) This means that IoT vendors may not have adequate awareness of privacy and security issues, or the expertise to address those issues.

Vendors and owners of IoT devices often have different expectations for how long a device will remain in service. A vendor may cease supporting a device, or a third party may discontinue a service on which the device depends,[[48]](#endnote-48) long before the device’s owner anticipates retiring the device.[[49]](#endnote-49) A vendor ceasing support for an IoT device can lead to greater privacy and security risks compared to traditional devices. Software usually becomes more vulnerable as it ages,[[50]](#endnote-50) and it is often impossible for entities other than the device’s manufacturer to access or modify an IoT device’s software or firmware. This can leave privacy issues and security vulnerabilities unfixable and potentially invisible to the owners of the devices.[[51]](#endnote-51)

Interoperability

The rapid expansion of the IoT in recent years has led to the development of many different kinds of devices, Application Programming Interfaces (**APIs**),[[52]](#endnote-52) infrastructure, data formats, standards and frameworks. This has caused significant interoperability issues, in that devices, software and data from one vendor often do not work with devices, software and data from other vendors.[[53]](#endnote-53)

Inconsistent APIs and data formats can cause problems with data portability, where the data of users or organisations is stored in vendor ‘silos’ that are incompatible with one another, making it difficult to transition from one vendor to another while keeping existing data.[[54]](#endnote-54) This lack of portability can lead to privacy and security issues. For example, if a smart city’s IoT vendor was found to have deceptively poor privacy practices, the city would face a choice between a potentially expensive struggle to transition to a new vendor, shutting down features or services of the city, or accepting that their citizens’ privacy may be interfered with.

These interoperability issues can also cause individuals to become ‘locked-in’ to a specific vendor. If every device in an individual’s smart home was from a single vendor, then that individual may be discouraged from purchasing a new device from a different vendor if it would be incompatible with their existing devices. In addition, the compatibility of devices can change over time as vendors support or lock-out other vendors.[[55]](#endnote-55)

Managing IoT devices

Many consumer IoT devices are ‘plug and play’, meaning that users are not required to configure them before use; they simply work out of the box. However, the default configurations of IoT devices tend to provide suboptimal privacy and security protections,[[56]](#endnote-56) and many users do not change settings from their defaults.[[57]](#endnote-57) In addition, consumers will not necessarily be aware that a device is an IoT device. An individual replacing their old refrigerator might not realise that their new refrigerator is an IoT device and may not fully understand the implications of that.

For organisations, a particularly problematic issue is that many IoT devices do not have centralised management features, and the devices that do have those features often do not follow any particular standard.[[58]](#endnote-58) This means that identical devices may need to be managed independently from one another, and devices from different manufacturers often need to be managed through different interfaces. This can cause significant challenges when managing IoT ecosystems at scale. When management options are not centralised or interoperable, the resources required to manage devices increases as the number and diversity of devices increases. If an organisation had thousands of devices from dozens of manufacturers, it would be near impossible to effectively manage them individually.

This issue can also apply to consumer devices, where it is common for devices to be managed by smartphone apps. If a person owns 10 IoT devices, they may require 10 different apps to manage them, likely leading to those devices being effectively unmanaged.

And when devices are not properly managed it can lead to privacy and security risks. For example, an organisation’s unmanaged device could continue to collect personal information after it is no longer needed for any purpose. Or, a device may not receive updates and become vulnerable to attack, allowing an intruder to access the rest of an organisation’s network, [[59]](#endnote-59) or use the device to disrupt the networks of other organisations.[[60]](#endnote-60)

IoT devices also generally provide less flexibility for administering or managing devices compared to traditional hardware. For example, it may be impossible for the owner of an IoT device to choose when to update the software of the device, with that decision restricted to the device’s manufacturer. Conversely, it may be impossible to use a device without updating it.

Accountability

The number of organisations that can be involved in an IoT ecosystem can make it difficult to identify who is, or should be, accountable for what. For example, an IoT camera could be owned by a local council, with data transmitted via a telecommunications company, stored by a cloud service provider, and accessed by law enforcement. Each entity in this example has some degree of responsibility for the personal information collected by the device, and it may be difficult for an individual to know who to contact if they wanted to request access to the information that the camera has collected about them.

The nature of IoT devices can make it impossible for an organisation to have control over every aspect of it. For example, organisations often have little or no control over security and privacy risks with communication technologies such as satellite or 5G, as these are usually provided by third party telecommunications companies. This can also be the case for cloud services, which can allow users to have anywhere from no control to high control over the security and privacy settings of services they are using.

It is also common for organisations to have unmanaged ‘rogue’ IoT devices connected to their networks.[[61]](#endnote-61) Employees can easily bring personal consumer IoT devices such as smart speakers or watches and connect them to the organisation’s network. Groups within an organisation can also install devices such as IoT televisions in meeting rooms or smart appliances in kitchens. These devices can pose privacy risks by, for example, collecting the personal information of unsuspecting employees, and can cause security risks by providing attackers with an easy entry point into an organisation’s network.[[62]](#endnote-62) These rogue IoT devices can be challenging for organisations as the individuals who should be accountable for them are often not aware of their presence.

Transparency

The passive nature of many IoT devices can make it difficult for individuals to be informed that their personal information is being collected. Devices in public spaces can collect information automatically, sometimes relying on individuals to opt-out if they do not want their information collected. But the non-interactive nature of many IoT devices makes it hard for opt-out models to work. Users may not be aware that their information is being collected, let alone that they can opt-out of that collection.[[63]](#endnote-63)

Additionally, when individuals want to inform themselves about what personal information a device collects and how that data is used, it can be difficult to find relevant information. IoT devices frequently do not have interfaces such as screens or input mechanisms such as keyboards, making it difficult for IoT devices to provide clarifying information like privacy policies. Instead, individuals are often required to navigate to the device manufacturer’s website or download an app. However, even when privacy policies for IoT devices are easily accessible, many of them do not provide sufficient information about how personal information is collected, used and disclosed.[[64]](#endnote-64)

The transparency of IoT devices could be further complicated by organisations seeking to use intellectual property rights to protect the way an IoT device collects or uses personal information, the data collected by devices, or the inferences and insights garnered from that data.[[65]](#endnote-65)

There are also challenges with individuals seeking access to their personal information collected by IoT devices. It cannot be assumed that an IoT device will have a single user, or that the user will own the device.[[66]](#endnote-66) This means that an IoT device can collect and store information about a range of people, and may allow users to access the personal information of other people.[[67]](#endnote-67) This is a difficult problem to solve as the lack of interfaces can make it difficult for devices to authenticate users to ensure they can only access information about themselves.

CONCLUSION

The IoT is expected to grow rapidly, increasingly connecting different aspects of our lives and further blurring the lines between online and offline worlds. Ultimately it is a tool that has the potential to bring benefits for everyone. However, the expansion of the IoT will allow for new kinds of personal information to be collected and increase the amount of personal information collected in general.

How this data is used will play a large part in how much good the IoT creates. Traditional methods used to protect privacy and better inform individuals about how their personal information is collected, used and disclosed are largely incompatible or insufficient for IoT devices. New and innovative solutions that can work with devices and services that essentially form infrastructure may be needed

Strong governance and transparency are also needed to reap the benefits of the IoT. Individuals should not have to choose between privacy and the convenience and efficiency of the IoT; it is essential that everyone be able to enjoy both.

1. Boyd Bangerter et al, ‘Networks and Devices for the 5G Era’ (2014) 52(2) *IEEE Communications Magazine* 90, available at: <https://pdfs.semanticscholar.org/c82b/071173279ec5501bc104cae3e3081b520be2.pdf>. [↑](#endnote-ref-1)
2. Rocco Di Taranto et al, ‘Location-aware Communications for 5G Networks’ (2014) 31(6) *IEEE Signal Processing Magazine* 201, available at: <http://publications.lib.chalmers.se/records/fulltext/208857/local_208857.pdf>. [↑](#endnote-ref-2)
3. See, for example, Andrew Raij et al, ‘Privacy Risks Emerging from the Adoption of Innocuous Wearable Sensors in the Mobile Environment’ (2011) *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 11, available at: <https://www.researchgate.net/publication/221518517_Privacy_risks_emerging_from_the_adoption_of_innocuous_wearable_sensors_in_the_mobile_environment>. [↑](#endnote-ref-3)
4. David Hall and James Llinas, ‘An Introduction to Multisensor Data Fusion’ (1997) 85(1) *Proceedings of the IEEE* 6, available at: <https://www.researchgate.net/publication/2985118_An_Introduction_to_Multisensor_Data_Fusion>. [↑](#endnote-ref-4)
5. Nashreen Nesa and Indrajit Banerjee, ‘IoT-based sensor data fusion for occupancy sensing using Dempster–Shafer evidence theory for smart buildings’ (2017) 4(5) *IEEE Internet of Things Journal* 1563. [↑](#endnote-ref-5)
6. Pardis Emami-Naeini et al, ‘Privacy Expectations and Preferences in an IoT World’ (2017) *Thirteenth Symposium on Usable Privacy and Security* 399, available at: <https://www.usenix.org/system/files/conference/soups2017/soups2017-naeini.pdf>. [↑](#endnote-ref-6)
7. See, for example, Ivan Mehta, ‘Amazon’s new patent will allow Alexa to detect a cough or a cold’ (15 October 2018) *The Next Web*, available at: <https://thenextweb.com/artificial-intelligence/2018/10/15/amazons-new-patent-will-allow-alexa-to-detect-your-illness/>. [↑](#endnote-ref-7)
8. N. Helberger, ‘Profiling and targeting consumers in the Internet of Things - A new challenge for consumer law’ (2016) *Digital Revolution: challenges for contract law in practice* 135, available at: <https://pure.uva.nl/ws/files/2802370/178742_1747.pdf>. [↑](#endnote-ref-8)
9. Explanatory Memorandum, Trade Practices Amendment (Australian Consumer Law) Bill (No.2) 2010 23.52, 465, available at: [https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/billhome/r4335%22](https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p%3Bquery%3DId%3A%22legislation/billhome/r4335%22). [↑](#endnote-ref-9)
10. Cheryl Dancey Balough, ‘Privacy Implications of Smart Meters’ (2010) 86(8) *Chicago-Kent Law Review* 161, available at: <http://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3780&context=cklawreview>. [↑](#endnote-ref-10)
11. S. Raj Rajagopalan et al, ‘Smart Meter Privacy: A Utility-Privacy Framework’ (2011) *2011 IEEE international Conference on Smart Grid Communications* 190, available at: <https://arxiv.org/pdf/1108.2234.pdf>. [↑](#endnote-ref-11)
12. Miro Enev et al, ‘Televisions, Video Privacy, and Powerline Electromagnetic Interference’ (2011) *Proceedings of the 18th ACM Conference on Computer and Communications Security* 537, available at: <https://homes.cs.washington.edu/~yoshi/papers/ccs2011-emi.pdf>. [↑](#endnote-ref-12)
13. United States National Institute of Standards and Technology, ‘Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid’ (2010), available at: <https://www.hsdl.org/?abstract&did=783017>. [↑](#endnote-ref-13)
14. See generally Liesbet van Zoonen, ‘Privacy concerns in smart cities’ (2016) 33(3) *Government Information Quarterly* 472, available at: <https://www.sciencedirect.com/science/article/pii/S0740624X16300818>. [↑](#endnote-ref-14)
15. Michel Foucault, ‘Discipline and Punish’ (1975); Ivan Manokha, ‘Surveillance, Panopticism, and Self-Discipline in the Digital Age’ (2018) 16(2) *Surveillance & Society* 219, available at: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/8346>. [↑](#endnote-ref-15)
16. Alice E Marwick and Danah Boyd, ‘I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience’ (2011) 13(1) *New Media & Society* 114; Sauvik Das and Adam Kramer, ‘Self-Censorship on Facebook’ (2013) *Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media*, available at: <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350>. [↑](#endnote-ref-16)
17. Ben Marder et al, ‘The extended “chilling” effect of Facebook: The cold reality of ubiquitous social networking’ (2016) 60 *Computers in Human Behavior* 582, available at: [https://www.researchgate.net/publication/296637938\_The\_extended\_'chilling'\_effect\_of\_Facebook\_The\_cold\_reality\_of\_ubiquitous\_social\_networking](https://www.researchgate.net/publication/296637938_The_extended_%27chilling%27_effect_of_Facebook_The_cold_reality_of_ubiquitous_social_networking). [↑](#endnote-ref-17)
18. Margot E. Kaminski, ‘Robots in the Home: What Will We Have Agreed To?’ (2015) 51 *Idaho Law Review* 661, available at: <https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2222&context=articles>. [↑](#endnote-ref-18)
19. Andria Cheng, ‘New York Proves Amazon Go Works, And An Even Bigger Rollout Is Only A Matter Of Time’ (26 June 2019) *Forbes*, available at: <https://www.forbes.com/sites/andriacheng/2019/06/26/amazon-gos-even-bigger-rollout-is-not-a-matter-of-if-but-when/#364b76f56f52>. [↑](#endnote-ref-19)
20. Organisation for Economic Co-operation and Development, ‘Personalised Pricing in the Digital Era’ (2018), available at: [https://one.oecd.org/document/DAF/COMP(2018)13/en/pdf](https://one.oecd.org/document/DAF/COMP%282018%2913/en/pdf). [↑](#endnote-ref-20)
21. Australian Competition and Consumer Commission, ‘Customer loyalty schemes’ (2019), available at: <https://www.accc.gov.au/publications/customer-loyalty-schemes-final-report>; Catherine Crump and Matthew Harwood, ‘Invasion of the Data Snatchers’ (25 March 2014) *American Civil Liberties Union*, available at: <https://www.aclu.org/blog/speakeasy/invasion-data-snatchers-big-data-and-internet-things-means-surveillance-everything>. [↑](#endnote-ref-21)
22. See, for example, City of Melbourne’s Pedestrian Counting System, available at: <https://www.melbourne.vic.gov.au/about-melbourne/research-and-statistics/city-population/Pages/pedestrian-counting-system.aspx>. [↑](#endnote-ref-22)
23. Scott R. Peppet, ‘Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent’ (2014) 93 *Texas Law Review* 85, available at: <https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf>. [↑](#endnote-ref-23)
24. See, for example, OVIC, ‘Disclosure of myki travel information: investigation report and compliance notice’ (2019), available at: <https://ovic.vic.gov.au/about-us/regulatory-action/investigations-audits-examinations/>. [↑](#endnote-ref-24)
25. See, for example, Yves-Alexandre de Montjoye et al, ‘Unique in the Crowd: The privacy bounds of human mobility’ (2013) 3 *Scientific Reports* 1376, available at: <https://www.nature.com/articles/srep01376.pdf>. [↑](#endnote-ref-25)
26. GSMA, ‘Protecting Privacy and Data in the Internet of Things’ (2019), available at: <https://www.gsma.com/iot/wp-content/uploads/2019/02/Protecting-Privacy-big-data-report-gsma.pdf>. [↑](#endnote-ref-26)
27. See, for example, Office of the Privacy Commissioner of Canada, ‘Investigation into the personal information handling practices of WhatsApp Inc.’ (2013) at 41, available at: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-001/>; FTC, ‘Does Hashing Make Data “Anonymous”?’ (2012), available at: <https://www.ftc.gov/news-events/blogs/techftc/2012/04/does-hashing-make-data-anonymous>; Paul Ducklin, ‘New York City makes a hash of taxi driver data disclosure’ (2014) *Naked Security by SOPHOS*, available at: <https://nakedsecurity.sophos.com/2014/06/24/new-york-city-makes-a-hash-of-taxi-driver-data-disclosure/>. [↑](#endnote-ref-27)
28. OVIC, ‘Protecting unit-record level personal information’ (2018), available at: <https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/>. [↑](#endnote-ref-28)
29. See, for example, Ilaria Torre et al, ‘Fitness Trackers and Wearable Devices: How to Prevent Inference Risks?’ (2017) *Proceedings of the 11th EAI International Conference on Body Area Networks* 125, available at: <https://www.researchgate.net/publication/316925412_Fitness_Trackers_and_Wearable_Devices_How_to_Prevent_Inference_Risks>. [↑](#endnote-ref-29)
30. Solon Barocas and Andrew D. Selbst, ‘Big Data’s Disparate Impact’ (2016) 104 *California Law Review* 671, available at: <http://www.californialawreview.org/wp-content/uploads/2016/06/2Barocas-Selbst.pdf>. [↑](#endnote-ref-30)
31. Reza Shokri et al, ‘Membership Inference Attacks Against Machine Learning Models’ (2017) *2017 IEEE Symposium on Security and Privacy* 3, available at: <https://www.cs.cornell.edu/~shmat/shmat_oak17.pdf>; Giuseppe Ateniese et al, ‘Hacking Smart Machines with Smarter Ones: How to Extract Meaningful Data from Machine Learning Classifiers’ (2013) 10(3) *International Journal of Security and Networks* 137, available at: <https://arxiv.org/abs/1306.4447v1>. [↑](#endnote-ref-31)
32. See, for example, MOTOsafety OBS GPS Tracker, available at <https://www.motosafety.com/features.html> [↑](#endnote-ref-32)
33. Meg Leta Jones, ‘Privacy Without Screens & the Internet of Other People's Things’ (2014) *Idaho Law Review* 639, available at: <https://www.uidaho.edu/-/media/UIdaho-Responsive/Files/law/law-review/articles/volume-51/51-3-jones-meg-leta.pdf>. [↑](#endnote-ref-33)
34. See, for example, Josh Bersin et al, ‘Will IoT technology bring us the quantified employee?’ (2016) *Deloitte*, available at: <https://www2.deloitte.com/us/en/insights/focus/internet-of-things/people-analytics-iot-human-resources.html>. [↑](#endnote-ref-34)
35. See, for example, Ceylan Yeginsu, ‘If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It)’ (1 February 2018) *The New York Times,* available at: <https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html>. [↑](#endnote-ref-35)
36. See, for example, Vivian Giang, ‘Companies Are Putting Sensors On Employees To Track Their Every Move’ (15 March 2013) *Business Insider*, available at: <https://www.businessinsider.com.au/tracking-employees-with-productivity-sensors-2013-3?r=US&IR=T>. [↑](#endnote-ref-36)
37. See, for example, Margaret Rhodes, ‘A Gadget Designed to Finally Make Doctors Wash Their Hands Enough’ (22 August 2014) *WIRED*, available at: <https://www.wired.com/2014/08/a-gadget-designed-to-finally-make-doctors-wash-their-hands-enough/>. [↑](#endnote-ref-37)
38. See, for example, Greg Kumparak, ‘Nest’s security system can now be a Google Assistant’ (5 February 2019) *Techcrunch*, available at: <https://techcrunch.com/2019/02/04/nests-security-system-can-now-be-a-google-assistant/>. [↑](#endnote-ref-38)
39. See, for example, Fergus Hunter, ‘”It is a stretch”: ACCC's Sims questions Google assurances over Fitbit data’ (19 November 2019), *The Sydney Morning Herald*, available at: <https://www.smh.com.au/politics/federal/it-is-a-stretch-accc-s-sims-questions-google-assurances-over-fitbit-data-20191119-p53by8.html>. [↑](#endnote-ref-39)
40. See, for example, Matt Day et al, ‘Amazon Workers Are Listening to What You Tell Alexa’ (11 April 2019) *Bloomberg*, available at: <https://www.bloomberg.com/news/articles/2019-04-10/is-anyone-listening-to-you-on-alexa-a-global-team-reviews-audio>; Sam Biddle, ‘For owners of Amazon’s Ring security cameras, strangers may have been watching too’ (11 January 2019) *The Intercept*, available at: <https://theintercept.com/2019/01/10/amazon-ring-security-camera/>. [↑](#endnote-ref-40)
41. Meredydd Williams et al, ‘The perfect storm: The privacy paradox and the Internet-of-Things’ (2016) *11th International Conference on Availability, Reliability and Security* 644*,* available at: <https://kar.kent.ac.uk/67485/1/ARES2016-author-final.pdf>. [↑](#endnote-ref-41)
42. Svetlana Yarosh and Pamela Zave, ‘Locked or Not? Mental Models of IoT Feature Interaction’ (2017) *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* 2993, available at: <http://www.pamelazave.com/yaroshCHI.pdf>; Sandra Spickard Prettyman et al, ‘Privacy and security in the brave new world: The use of multiple mental models’ (2015) *International Conference on Human Aspects of Information Security, Privacy, and Trust* 260. [↑](#endnote-ref-42)
43. Manuel Silverio-Fernández et al, ‘What is a smart device? - a conceptualisation within the paradigm of the internet of things’ (2018) 6(1) *Visualization in Engineering* 3, available at: [https://link.springer.com/content/pdf/10.1186%2Fs40327-018-0063-8.pdf](https://link.springer.com/content/pdf/10.1186/s40327-018-0063-8.pdf); Stephan Haller, ‘The Things in the Internet of Things’ (2010) 5(8) *Internet of Things Conference 2010* 26, available at: <https://www.researchgate.net/publication/228488111_The_Things_in_the_Internet_of_Things>. [↑](#endnote-ref-43)
44. Eric Horvitz and Deirdre Mulligan, ‘Data, privacy, and the greater good’ (2015) 349(26245) *Science* 253. [↑](#endnote-ref-44)
45. See generally Jon Gold, ‘IoT in 2020: The awkward teenage years’ (15 November 2019) *Networkword*, available at: <https://www.networkworld.com/article/3453643/iot-in-2020-the-awkward-teenage-years.html>. [↑](#endnote-ref-45)
46. Yu Tianlong et al, ‘Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things’ (2015) *Proceedings of the 14th ACM Workshop on Hot Topics in Networks* 5, available at: <https://www.cs.cmu.edu/~srini/papers/2015.Yu.hotnets.pdf>; Bruce Schneier, ‘Click Here to Kill Everyone’ (27 January 2017) *New York Magazine*, available at: <https://nymag.com/intelligencer/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html>. [↑](#endnote-ref-46)
47. See generally Brian Fung, ‘Here’s the scariest part about the Internet of Things’ (19 November 2013) *Washington Post*, available at: <https://www.washingtonpost.com/news/the-switch/wp/2013/11/19/heres-the-scariest-part-about-the-internet-of-things/?arc404=true>. [↑](#endnote-ref-47)
48. See, for example, Lorenzo Franceschi-Bicchierai ‘Smart Fridge Only Capable of Displaying Buggy Future of the Internet of Things’ (12 December 2015) *Vice*, available at: <https://www.vice.com/en_us/article/aekdkp/smart-fridge-only-capable-of-displaying-buggy-future-of-the-internet-of-things>. [↑](#endnote-ref-48)
49. See, for example, Nick Statt, ‘Nest is permanently disabling the Revolv smart home hub’ (4 April 2016) *The Verge*, available at: <https://www.theverge.com/2016/4/4/11362928/google-nest-revolv-shutdown-smart-home-products>. [↑](#endnote-ref-49)
50. Sandy Clark et al, ‘Familiarity Breeds Contempt: The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities’ (2010) *Proceedings of the 26th Annual Computer Security Applications Conference* 251, available at: <https://www.researchgate.net/publication/221046575_Familiarity_breeds_contempt_The_honeymoon_effect_and_the_role_of_legacy_code_in_zero-day_vulnerabilities>. [↑](#endnote-ref-50)
51. See generally Bruce Schneir, ‘The Internet of Things Is Wildly Insecure — And Often Unpatchable’ (6 January 2014) *WIRED*, available at: <https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/>. [↑](#endnote-ref-51)
52. An API is a way for a computer to communicate with another computer, or for a person to interrogate or instruct a computer and get a result. [↑](#endnote-ref-52)
53. Mahda Noura et al, ‘Interoperability in Internet of Things: Taxonomies and Open Challenges’, (2019) 24(3) *Mobile Networks and Applications* 796, available at: <https://link.springer.com/article/10.1007/s11036-018-1089-9>. [↑](#endnote-ref-53)
54. Justice Opara-Martins et al, ‘Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective’ (2016) 5(1) *Journal of Cloud Computing: Advances, Systems and Applications 4*, available at: <https://link.springer.com/article/10.1186/s13677-016-0054-z>. [↑](#endnote-ref-54)
55. See, for example, Ry Crist, ‘Philips Hue cuts support for third-party bulbs’ (14 December 2015) *CNET*, available at: <https://www.cnet.com/news/philips-hue-cuts-support-for-third-party-bulbs/>. [↑](#endnote-ref-55)
56. Meredydd Williams et al, ‘The perfect storm: The privacy paradox and the Internet-of-Things’ (2016) *11th International Conference on Availability, Reliability and Security* 644*,* available at: <https://kar.kent.ac.uk/67485/1/ARES2016-author-final.pdf>; Brian Krebs, ‘IoT Reality: Smart Devices, Dumb Defaults’ (18 February 2016) *Krebs on Security*, available at: <https://krebsonsecurity.com/2016/02/iot-reality-smart-devices-dumb-defaults/>. [↑](#endnote-ref-56)
57. Wendy E. Mackay, ‘Triggers and barriers to customizing software’ (1991) *Proceedings of the SIGCHI conference on Human factors in computing systems* 153; Ralph Gross and Alessandro Acquisti, ‘Information Revelation and Privacy in Online Social Networks’ *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* 71; Cf Danah Boyd and Eszter Hargittai, ‘Facebook privacy settings: Who cares?’ (2010) 15(8) *First Monday*, available at: <https://firstmonday.org/ojs/index.php/fm/article/view/3086/2589>. [↑](#endnote-ref-57)
58. Katie Boeckl et al, ‘Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks**’** (2018) *National Institute of Standards and Technology*, available at: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf>. [↑](#endnote-ref-58)
59. Michael J. Covington and Rush Carskadden, ‘Threat Implications of the Internet of Things’ (2013) *5th International Conference on Cyber Conflict*1, available at: <https://ccdcoe.org/uploads/2018/10/1_d1r1s6_covington.pdf>. [↑](#endnote-ref-59)
60. See, for example, Ben Herzberg et al, ‘Breaking Down Mirai: An IoT DDoS Botnet Analysis’ (26 October 2016) *Imperva*, available at: <https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/>. [↑](#endnote-ref-60)
61. Infoblox, ‘Infoblox research finds explosion of personal and IoT devices on enterprise networks introduces immense security risk’ (2018), available at: <https://www.infoblox.com/company/news-events/press-releases/infoblox-research-finds-explosion-of-personal-and-iot-devices-on-enterprise-networks-introduces-immense-security-risk/>. [↑](#endnote-ref-61)
62. See, for example, Oscar Williams-Grut, ‘Hackers stole a casino's high-roller database through a thermometer in the lobby fish tank’ (16 April 2018) *Business Insider*, available at: <https://www.businessinsider.com.au/hackers-stole-a-casinos-database-through-a-thermometer-in-the-lobby-fish-tank-2018-4>. [↑](#endnote-ref-62)
63. See, for example, In the matter of Nomi Technologies, Inc (United States of America Before the Federal Trade Commission, Docket No. C-4538, 28 August 2015), available at: <https://www.ftc.gov/system/files/documents/cases/150902nomitechcmpt.pdf>. [↑](#endnote-ref-63)
64. Office of the Australian Information Commissioner, ‘Privacy Commissioners reveal the hidden risks of the Internet of Things’ (2016), available at: <https://www.oaic.gov.au/updates/news-and-media/privacy-commissioners-reveal-the-hidden-risks-of-the-internet-of-things/>. [↑](#endnote-ref-64)
65. IP Australia, ‘IP Australia and the Future of Intellectual Property’ (2017), available at: <https://www.ipaustralia.gov.au/sites/default/files/ip_australia_and_the_future_of_intellectual_property.pdf>; Alexandru Serbanati et al, ‘Building Blocks of the Internet of Things: State of the Art and Beyond’ (2011) *Deploying RFID-Challenges, Solutions, and Open Issues*, available at: <https://www.intechopen.com/books/deploying-rfid-challenges-solutions-and-open-issues/building-blocks-of-the-internet-of-things-state-of-the-art-and-beyond>. [↑](#endnote-ref-65)
66. Amardeo Sarma and João Girão, ‘Identities in the Future Internet of Things’ (2009) 49(3) *Wireless Personal Communications* 353, available at: <https://www.researchgate.net/publication/226218872_Identities_in_the_Future_Internet_of_Things>. [↑](#endnote-ref-66)
67. Christine Geeng and Franziska Roesner, ‘Who’s In Control?: Interactions In Multi-User Smart Homes’ (2019) 268 *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* 1, available at: <https://www.franziroesner.com/pdf/geeng-smarthomes-chi19.pdf>.

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice. [↑](#endnote-ref-67)