Chapter 3
Privacy in the New Age of IoT

Qi Pan

3.1 Introduction

Our daily lives are becoming increasingly digitised. The line between our offline and online presence is blurring as consumers and organisations rely on digital devices to stay connected and efficient. As a result, the concept of privacy, defined by the Oxford English Dictionary as "a state in which one is not observed or disturbed by other people", is shifting. The preferences of individuals are tracked, health data is monitored, and all of this data can be collected and mined by organisations who monetise data through targeted advertising and third party sharing, and governments who track individuals. The Internet of Things (IoT) is defined as systems of sensors and actuators connected by networks to computing systems, and it relies on a backbone of connectivity and interoperability. As Hugh Durrant-Whyte stated at the Royal Society conference entitled "IoT: Opportunities and threats" on 3 October 2017, the main impact of IoT is in data and how it is used, not in the physical devices which can become obsolete over time [1]. In the past, data was captured and transferred freely from consumers, often in order to receive targeted offers or an improved credit rating. The control of the data lay with the organisations who freely shared this data. However, in the aftermath of the Facebook/Cambridge Analytica scandal, news of which broke in March 2018, light has been shed on the misuse of personal data and the breach of privacy by organisations consumers entrust with their data [2].

In the context of IoT, there are two major risks associated with privacy. The first and more pertinent risk is the privacy associated with consumer and employee data captured from IoT sensors in devices such as wearables, virtual assistants, such as Alexa, and smart cars. The second risk is related to the proprietary information held

Q. Pan (✉)
London, UK
e-mail: qi.pan@hotmail.co.uk

F. D. Hudson (ed.), *Women Securing the Future with TIPPSS for IoT*, Women in Engineering and Science, https://doi.org/10.1007/978-3-030-15705-0_3

by organisations, which can be compromised in the event of a data breach. The impacts of the lack of privacy on individuals and companies are wide-reaching and range from reputational damage to extreme governmental surveillance.

Policymakers are in a never-ending rat race with technological innovation, and all the while IoT is becoming more widespread and affordable. The European Union's (EU's) General Data Protection Regulation (GDPR) empowers data subjects to have more visibility and control over their data and exercise their rights over it, which has significant implications for businesses and organisations large and small. Not only will the GDPR increase transparency and trust between data owners and subjects, but it will also encourage data controllers to think more closely about the legitimate business purpose of collecting the data and sharing it with third parties. It is only a matter of time before other nations adopt a similar standard for data protection.

In the future, individuals will need to take more ownership of their own data and understand what they are agreeing to in user agreements and privacy policies. This requires technology companies to be more transparent and educate their data subjects in plain language. Although disruption is key to IoT innovation and has potential far-reaching benefits including improved health and well-being and improved traffic flow, privacy by design is critical in ensuring the trust of consumers and avoiding potential personal or professional risks.

3.2 Data is at the Core of Privacy and IoT

3.2.1 What is Privacy?

> *Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech* [3].

If a stranger asked you about your health and well-being, what you last bought on Amazon, and followed you around town, that might feel like an invasion of privacy. However, social media and apps constantly monitor and share your preferences in order to target your profile, and fitness tracking apps, such as Strava and Nike Run Club, monitor your location. In the new digital age, as the separation of online and offline is diminishing, it is hard to feel truly alone or private. One must question if consumers really want privacy. Digital natives have grown up with a wealth of information at their fingertips, and with virtual friendships rather than physical ones. According to Childwise, the average time spent in front of a screen, doing anything from playing games on a tablet to watching TV, increased from 3 h in 1995 to 6½ h in 2015 [4]. During that period of technological advancement, privacy was not at the forefront of people's minds. Consumers tend to want the newest gadget; a study from Barclays found that 62% of consumers would upgrade their smartphone in the next year [5]. Privacy in the context of IoT is a relatively new topic, but one that will become more pertinent as consumer adoption of IoT devices grows.

3.2.2 IoT and Data

Each IoT device has a unique ID and Internet Protocol (IP) address. Sensors in devices monitor the environment and humans in that environment, be it voice, temperature or blood sugar level. This sensor data is captured in microchips in the devices, which communicate to other devices on a network using Radio frequency identification (RFID) and Near-field communication (NFC). The data is then subjected to analytics to drive insights and actions. Actions could range from recommending a product to a consumer to increasing insulin levels in the bloodstream. Data is key for IoT, and can be broadly categorised into two buckets: personal data (including sensitive personal data), and non-personal data, which includes both proprietary data belonging to businesses, and open data such as traffic data. Companies that collect IoT data often harness it in data lakes or data fabrics, normally not making full use of the data and storing it indefinitely. Machine-learning algorithms are then applied to the big data in order to profile the users, drive insights and make recommendations. This can benefit consumers and corporations alike, increasing convenience for purchasing decisions, or creating medical recommendations. For example, Google revealed a way of using machine learning to personalise search ads to target consumers in 2018 [6].

IoT can itself be separated into two main buckets: the Internet of Humans, and the Internet of Machines. In the Internet of Humans, consumers freely share data with IoT devices to reap the benefits, often oblivious to the downstream implications of their data usage. Having a vast repository of personal data also allows companies to assign attributes to personas. Based on these personas, companies can then target individuals with information or advertising. IoT devices collect not only consumer data, but also employee data and proprietary business data, which is part of the Internet of Machines. The smart industry, or Industry 4.0, involves machine to machine (M2M) IoT device communications. Proprietary data captured from IoT devices could be highly confidential and contain intellectual property. Where confidential information is shared by organisations via an IoT network, this data could also be the subject of tampering or hacking; for example, the breach of this data could compromise a competitive advantage or give a competitor a head start in the race for a patent approval.

3.2.3 Data Considerations

A key challenge with the process of gaining insights from data is data quality. Companies often collect data without verification or deduplication (removing duplicate data entries). As such, data governance is key to ensuring one source of truth when it comes to personal data. Once this data is captured, much of the data is often left untouched, leading us to the question of why is it captured in the first place. According to a McKinsey Global Institute report, less than 1% of IoT data is

currently used [7]. Organisations need to be more mindful about the personal data they capture on individuals in two ways. Firstly, they should only capture the data needed, and be selective over where this data is transferred, preventing unnecessary future complications. Secondly, if the data is no longer useful, then it should be deleted unless it is the subject of a litigation hold. If data is shared with multiple third parties, it is harder for the data to be deleted should the consumer exercise their right to request it. To make the deletion process easier, the data controller should map where the data flows. Transparency between data owner and data controller and data subject is key for IoT uptake.

3.3 Use Cases of Privacy and IoT

The Panopticon can be used as a metaphor for Privacy in the context of IoT. Jeremy Bentham's Panopticon is a building where a watchman in a tower watches the inhabitants in cells who do not know whether or not they are being watched at any time. The French philosopher Michel Foucault used it as an example of asymmetrical surveillance. "He is seen, but he does not see; he is an object of information, never a subject in communication" [8]. However, whereas in the Panopticon the inhabitants are aware of the possibility of being watched, in the digital age, there is no watchtower looming over us when we say "Alexa, switch off the lights". In this situation, the providers of IoT devices are the watchman, and the IoT devices are the watchtower. A stark parallel can thus be drawn between the Panopticon and IoT. Rather than our physical bodies being watched by a watchman, our actions and decisions are being captured as data not only by the government, but by corporations who create personas according to the data. At the extreme end of the spectrum, we are living in a surveillance state, or a digital panopticon (Fig. 3.1).

Time	***7 am***	***7:30 am***	***8 am***	***9 am to 5 pm***	***6 pm***	***24/7***
Context	Switch on the kettle	Morning run	Drive to work	At work	Evening in	Always-on
IoT Device	Alexa	Fitbit	CCTV	Implanted chips	Smart TV	Pacemaker
Sensor	Voice	Heart rate	License number plate	Location	Voice	Heart rate
Output	Kettle	Data	Crime monitoring	Increased efficiency	Ease of use	Healthcare

Fig. 3.1 A day in the life of IoT

3.3.1 Consumer Industry

In the consumer industry, corporations use Data Management Platforms to trace clicks from any devices, thus following a consumer journey, and can target with advertisements based on one's persona and device to ensure their product is at the forefront of the mind and easy to purchase. This becomes even more pertinent when devices such as Alexa, Amazon's cloud-based virtual assistant, are added to the mix. Rather than physically tapping a touchscreen, what if Alexa hears your conversations and recommends products to you? What if a wearable health device detects the symptoms of a disease and tells your phone to advertise the treatment for it on your Instagram, or on a loved one's Facebook? Although both potential situations may benefit the consumer in terms of convenience, there must be a balance between ease of purchase and personal privacy. The impact of a lack of privacy can affect more than just the end user. The Strava fitness tracker app uses GPS tracking to calculate distance travelled and elevation gained. Although these routes are not public, the app also provides a publicly available heat map that shows the exercise routes of all users. The users are all anonymised, but still the heat map inadvertently put lives at risk by sharing the routes of soldiers in secret military bases [9].

3.3.2 IoT for Healthcare

In the healthcare sector, personal medical devices are hailed as putting the control of healthcare in the hands of the patients. The role reversal of patients becoming teachers and doctors students is transforming the healthcare industry. Examples of this role reversal in action range from simple iPhone apps such as Ada Health which use artificial intelligence to analyse your symptoms and suggest disease states and treatments, to wearable devices which monitor your health remotely, providing real time feedback and potentially decreasing medical costs and the need for hospital beds. The benefit of having all of this data about yourself is also a risk. Whereas in the past, you would go to your doctor to have a test taken, which would be recorded on paper or a local computer (mainframe), these days, many of the solutions rely on Software as a Service (SaaS) or Platform as a Service (PaaS) solutions. In order to analyse the data and drive recommendations, the data captured from the device is sent to the "Cloud" where it is analysed. The output is then pushed back to the device. The risk here stems not only from the likelihood of the network of the IoT being hacked, but also by it being manipulated or stolen. For example, if a hacker is able to access the cloud where your medical information is held, they can one, hold it to ransom, as happened as part of the global cyberattack by WannaCry in 2017 [10], two, manipulate it to alter the dosage of drugs to potential toxic levels, three, sell it to unethical third parties and research companies, or four, use it for identity theft. These issues can all stem from a lack of privacy and security standards.

In April 2018, some 350,000 patients with a cardiac defibrillator were told that their devices were vulnerable to cybersecurity attacks [11]. The devices, manufactured by St Jude's Medical (which was acquired by Abbott Laboratories in January 2017), needed to have a firmware update, which required patients to visit their healthcare providers to get an upgrade. Prior to this, St Jude's was embroiled in another scandal in which the IoT company MedSec found vulnerabilities in the devices which could be life-threatening if hacked. St Jude's subsequently applied updates to the Merlin remote monitoring system, which is connected to cardiac devices [12]. Merlin.net is a patient care network, which works together with Merlin@home, a transmitter which monitors the device and sends the information to the doctor, reducing hospital visits. Many of the 350,000 patients are likely to be elderly, and may not understand the significance of malware patches and the risks associated with taking no action. Thus, it is the responsibility of the device manufacturers to clearly state the risks associated and effectively communicate this to the patients and doctors.

3.3.3 Smart Homes

IoT extends further than just wearable devices. Smart homes and offices have been hailed as a way to increase energy efficiency thanks to smart meters and sensors which detect your presence and alter the thermostat or lighting accordingly. An example of this is the remotely operated smart thermostat developed by Nest Labs, which uses machine learning on data captured from sensors to track people's schedules and adapt the temperature of their environment accordingly to conserve energy. Nest Labs is a smart automation company founded by Apple engineers and acquired by Google in 2014. In May of the same year, activists from the German group Peng! Collective pretended to be Google representatives to unveil a new site Google Nest at the Re:public tech conference. Google Nest used Google's iconography to poke fun at its privacy policies, and offered four products that were unnervingly believable [13]. All four products captured personal information for different purposes:

- Google Trust "The more Google products you use, the higher your insurance payout will be in case of data misuse through secret service or private criminals."
- Google Hug: "Google Hug helps you find others nearby who have the same needs you do."
- Google Bee: "Introducing the first personal drone. Google Bee watches over your house and family when you are away".
- Google Bye, a memorial site: "Each time you use a Google service, like downloading an app from the Play Store or watching a video on YouTube, you tell us a little bit more about yourself. Why leave that valuable information with us when you can share it with others?"

The site was so convincing that people emailed it asking for more information about the features offered.

The concerns associated with lack of privacy can be manipulated not only by individuals and organisations, but also by governments. In 2017, Wikileaks revealed that the US Central Intelligence Agency (CIA) had tapped into smart devices, including Samsung's smart TVs. In leaked notes from a "Weeping Angel" workshop the CIA conducted with the UK's Security Service (MI5), detailed instructions were given about software which enabled a Fake-Off mode. This allowed the CIA to listen in to conversations and send them to a CIA server, even when the TV is apparently switched off, and included "Suppress LEDs" to make the Fake-Off mode look better [14]. Michael Hayden, an ex-CIA director responded to this by trying to reassure citizens: "These tools would not be used against an American", and "There are bad people in the world that have Samsung TVs, too" [15]. This begs the questions: are all Americans good? What defines an American?

3.3.4 Smart Offices

Security is an advantage that comes with smart homes and offices; the McKinsey Global Institute (MGI) states that "by using digital security cameras with advanced image-processing capabilities, operators of office buildings can monitor activity throughout their properties without requiring guards to patrol or continuously monitor video feeds" [7]. In workplaces, IoT can track workers in real time to warn them when they are entering an area of concern, and some modern employers are also using IoT to increase efficiency by tracking employees. In Sweden, the technologically advanced company Epicenter put RFID chips under the skin of staff to enable them to gain access to the building or use the photocopier [16]. Although this is improving safety and efficiency, this is a prime example of forsaking privacy for extreme convenience.

3.3.5 Smart Cities and Crime

At a higher level, smart cities will offer improved transportation efficiency. By putting IoT devices on public transport vehicles, the location of each vehicle can be tracked at any point in time, telling you how far away your bus is. By tapping your pass on the bus, your location can also be mapped to that bus. Some governments are also tracking vehicle license plates using cameras to catch drivers who are speeding. In these situations, there is no process in place to gather consent from the drivers.

Privacy becomes more muddied in the context of communities. The Baltimore Police Department deployed Cessna airplanes with surveillance cameras to fly over the streets of Baltimore with the purpose of monitoring crime, to the ignorance of

innocent civilians [17]. As such, the move to smart homes and smart cities raises concerns about transparency. In Toronto, Canada, Google's parent company Alphabet is pioneering Sidewalk Labs in Quayside on the banks of Lake Ontario [18]. Canadian Prime Minister Justin Trudeau coined it as a "thriving hub for innovation, [to] create the good, well-paying jobs that Canadians need." Sidewalk Labs boasts automatic waste collection, autonomous vehicles and connected transit systems. Google called it "a distributed network of sensors to collect real-time data about the surrounding environment." How will this work in terms of privacy? With facial recognition on the streets, thoughts will be the only thing which will remain private, especially since eye-tracking software can already detect an individual's mood solely based on facial movements. Will a privacy notice be served to the residents every time a new IoT device is deployed?

3.3.6 Protecting Privacy

A new trend of Edge Analytics has the potential to curb many of these risks described. Edge analytics relies on the local computing power of the IoT device and other devices closer to the edge of the network, rather than that of the cloud network. If analytics and decision making can be done locally, then this mitigates the risks associated with the cloud being hacked. In addition, the local hosting of data leads to increased data privacy, a decreased risk of hacking, and increased data ownership by the consumer rather than the supplier. Of course, there is still the possibility of the device itself being breached; however, this is less favourable for hackers than breaching a single point of security which touches multiple users. Blockchain also has the potential to increase privacy in IoT. Rather than sending data to a central corporate-owned cloud, what if the data was decentralised? This way, only metadata containing no personal information is transferred between systems.

The importance of privacy can be found in many use cases for IoT, as discussed. The movements and decisions humans make are datafied by IoT, and IoT can subsequently dictate our next actions. Consumers can reap benefits from IoT in their daily lives. For example, Alexa listens to commands which can control the lighting in your house to go the time you wake up in the morning. Alexa can also connect to smart automated home systems such as your smart kettle. As a McKinsey Global Institute paper on IoT states, the opportunities of IoT in the home can give consumers time back due to the automation of domestic chores, and increase energy efficiency [7]. The variety of use cases requires privacy standards which can be applied to all these situations. It is time suppliers begin to share best practice in ensuring the privacy of users is respected. Proportionality is required to ensure technological innovation can proceed. One way in which this can be done is by categorising personal data depending on its sensitivity, and putting in suitable controls based on that category of data.

3.4 The impacts of Privacy (or Lack Thereof) on Our Daily Lives

3.4.1 Consumer Demand for IoT

Philip N Howard writes in his book *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* that the Internet of Things will lead to a new political age he calls the "Pax Technica", where the government and technology companies have hegemony over citizens [19]. However, the societal impact of privacy is yet to emerge in full force. This is due to the relatively slow uptake of smart devices by consumers. Only 6% of American households have a smart-home device, including internet-connected appliances, home-monitoring systems, speakers or lighting, according to Frank Gillett of Forrester, a research firm. A survey conducted by PricewaterhouseCoopers found that 72% of people did not expect to adopt smart-home technology over the next 2–5 years. Forrester predicts that growth will be slow, with around 16% of American households with a smart-home device in 2021 [20]. The reason for this can be boiled down to the cost of the devices combined with the lack of necessity. A Samsung fridge costs $5000, and do you really need to check what is left in the fridge without opening the door? The Economist also attributes the slow uptake to the low turnover of smart-home devices. The smart-device ecosystem is still disparate, and in order for it to be successful, more interoperability on open platforms is needed.

3.4.2 Consumer Privacy

The Amazon Echo is an example of a smart device that is performing well. The success of the Amazon Echo is due to the affordability of the Echo device and its commerce revenue stream. The investment firm Mizuho predicts that by 2020, $4 billion will come from the sales of the Echo devices, and a whopping $7 billion Echo related revenue generated from the commerce on Amazon.com [21]. Amazon is an example of a company which excels at customer engagement and retainment, and prides itself on its customer obsession. When a consumer searches for a product on Amazon, he/she receives email reminders from Amazon, and advertisements on other websites, pushing the product to the forefront of the consumer's mind. Although Amazon states that Echo devices do not listen in to all conversations, and only listen when the word Alexa is used, it emerged in May 2018 that a private conversation between a lady called Danielle and her husband was recorded and sent to a random contact, without consent [22]. Fortunately, the conversation was about hardwood flooring. Nevertheless, Danielle called it "a total privacy invasion. Immediately, I said, 'I'm never plugging that device in again because I can't trust it.'" Although in this situation, Amazon claimed it was an extremely rare occurrence due to Alexa mishearing trigger words rather than listening to all conversations,

Amazon has filed patent applications for "voice-sniffing" algorithms which constantly listen for words such as "love" and if they "bought" something, analyse the speech, adding it to a database [23]. Following this, the patent application even goes on to propose a way to serve targeted advertisements to not only the consumers themselves but also their friends and family members.

Amazon's motivations outlined above raise many questions about privacy, which the more vulnerable members of the population are not asking. In particular, the elderly, who grew up during a time before the internet was invented, may not appreciate how to protect their privacy online. There is a whole host of new terminology constantly being birthed, often by millennials, which can be hard to keep up with and understand. "We use cookies to provide you with the best experience on our site" is a common phrase found on most websites. Many people do not know that cookies capture site name and a unique user ID, meaning that when you visit the website again, your PC tells the site, which can then personalise the content based on previous visits. Some cookies are more sophisticated. They might record how long you spend on each page on a site, what links you click, even your preferences for page layouts and colour schemes. They can even be used to store data on what is in your "shopping cart". This means that you could receive targeted offers based on your browsing history. The new EU ePrivacy regulation, which is yet to be implemented, explicitly points to IoT in the proposal "the principle of confidentiality which is enshrined in the Regulation should also apply to the transmission of machine-to-machine communications [24]." The ePrivacy Regulation aims to simplify rules governing cookies, and gives individuals more rights around electronic communications.

3.4.3 Privacy Education

The lack of general understanding around technology in society has led to many consumers being oblivious to the lack of data privacy, and at the other extreme, technophobes. As such, education is key in ensuring a balanced approach to the use of technology in our daily lives. With attention spans decreasing, we are unlikely to read through the privacy notice on websites, or change our privacy settings on Facebook. Often, it is only when a breach of privacy occurs, that action to protect privacy is taken. More needs to be done by regulators and technology companies to communicate how to protect privacy in a way that is intelligible by society. The way that this is done is also crucial. Rather than having pages of long documentation, regulators and technology firms should use their abundant innovative resources and invest in new ways to capture the attention of consumers using modern communication channels, such as infographics, videos and virtual reality. Facebook has done this by sharing bite-size clips about their privacy settings, and advertising on billboards; however, it may be too little, too late for them. Only once individuals truly understand how their data is being processed, will they take ownership and accountability over it. If identity theft and catfishing, which is where someone pretends to

be another person online to date someone, can occur from data captured on personal computers (PCs), the risk becomes even greater if hackers can access smart devices.

3.4.4 Societal Impacts and Discrimination

"Nudge theory" is a behavioural psychology concept explained in the book *Nudge: Improving Decisions About Health, Wealth, and Happiness* by Richard Thaler and Cass Sunstein and involves adapting the environment to trigger cognitive processes [25]. Wearable devices such as Fitbits and Apple Watches claim to help consumers reach their health and fitness goals. One major motivating factor for individuals to exercise more is the community aspect. Some people do not go for a run unless they have Strava switched on, so they can share their exercise with others. This is an example of positive data sharing. The gamification of fitness using apps brings out the competitive nature of individuals, such as various step challenges where different teams compete to rack up the most steps.

Conversely, the rise in technology has also been blamed as a major cause of the incidence of increasing mental health issues. The herd nature of social media can give strength to those who have the same opinions, but also alienate individuals with differing opinions, and this can be perpetuated by the community aspect of wearable devices. Having your data out in the open leaves it open to judgement and profiling. However, some digital natives are defying the norm and generating new ways to succeed in the modern world, and there are ways in which IoT can combat these issues. In 2017, school children came together in the UK to develop ways to do this. Innovative ideas include a smart wearable band "Breath Watch: a wristband that monitors the symptoms of a panic attack and provides calming down techniques via a mobile phone or tablet [26]." Interestingly, Public Health Canada takes advantage of the lack of online privacy by combing social media posts for indicators of mental health and likelihood of suicide [27].

The lack of privacy associated with sensitive personal data such as medical data captured from wearable devices can have a detrimental impact on insurance and employability. Even non-sensitive personal data can lead to discrimination. Lawyers in the USA have used big data and machine learning to calculate the probability of criminals reoffending, and police in the UK have used technology for "predictive crime mapping" [28, 29]. Although these examples are in the best interests of ensuring citizens' safety, one of the biggest markers of likelihood of crime and reoffending was location and race. Because the data used to train the algorithm was inherently biased, the algorithm learned and reinforced racial bias, effectively discriminating against certain races. Currently, the algorithms use crime type, location, date and time; however, the potential of adding data captured from IoT devices to the mix could raise more controversial issues. In these hypothetical circumstances, it is important to distinguish between correlation and causation.

3.4.5 Governmental Monitoring

The lack of privacy can be manipulated by governments, as well as individuals, and organisations. In 2013, Edward Snowden revealed the state of extreme surveillance engineered by the US government, alongside the UK, Australia and Canada [30]. The National Security Agency (NSA) was able to access Google and Yahoo accounts as well as phone calls, and thus snoop on citizens' personal and professional lives. Ironically however, the documents which showed the lack of privacy, also inadvertently breached the privacy of agents, forcing them to move location for their security. In 2016, The Guardian released an article where James Clapper, the US director of national intelligence, confessed that "in the future, intelligence services might use [IoT] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials" [31]. Despite all of this, there is no single federal law regulating collection and use of personal data in the USA as of 2018.

3.5 Privacy Regulations and Their Implications for Organisations and Individuals

The Cambridge Analytica data scandal, among others, have highlighted the importance of data protection in the digital age where technology is advancing at a rapid pace and data is becoming the new oil, both by fueling the economy of the future and increasing in value. Websites, including the big tech giants, feed off consumer data to generate revenue from targeted advertising, and this often benefits consumers, who can get attractive deals relevant to them. The risk lies when the data is misused or breached, and consumers are at the mercy of the data controller.

3.5.1 The EU General Data Protection Regulation

The EU General Data Protection Regulation (GDPR) puts control back in the hands of consumers. It came into effect on 25 May 2018, and aims to harmonise data protection laws across the EU and give regulators stronger enforcement powers. The same rules apply to international companies who process EU personal data, and this led to the EU-wide shutdown of websites such as the LA Times who were not ready for the deadline [32]. On the plus side, others are now using the GDPR as best practice, with the Salesforce CEO Marc Benioff saying that the USA should follow suit and implement a similar data privacy law [33]. The GDPR applies to IoT, as it mentions RFID tags in its list of online identifiers. There are two main ways the GDPR is empowering consumers: through increased transparency, and bolstered consumer rights. The tirade of emails asking us to keep in touch have been a direct result of

the GDPR requirement to serve a privacy notice and ask for explicit, opt-in consent where legally required. This requirement is a great start in encouraging companies to consider and clearly communicate what data they are capturing (data minimisation), what they are using the data for, and how long they are keeping the data (retention policies). The burden of increased scrutiny and tighter regulations has meant that organisations tend to capture less sensitive personal information, unless it is crucial. GDPR has brought to light the wealth of archived and unused data, and led to a conscious decision to either contact the data subject to keep storing the data, or undergo a spring clean of the unused data.

The GDPR is a great first step in regulating data processors, but it is important to be realistic about the benefits. An example of this is Article 13 of the GDPR "Information to be provided where personal data are collected from the data subject" which refers to a privacy notice [34]. According to Emily Taylor, associate fellow of Chatham House, it would take 250 h per year to read all of the privacy notices of services from start to end [35]. Consumers tend to choose convenience over control. When you are in a foreign location, it is easy to reach for your phone and see what restaurants are nearby, and how to get there. As such, it is important for companies to show that they value their consumers' data rights by making the privacy notice more easily accessible, and clearly stating which second and third parties process the data.

A common misunderstanding about the GDPR is that consent is required for processing data. Consent is only required where there is no legitimate business purpose for processing the data, such as for direct marketing purposes. This becomes tricky in some situations, such as a retail context where a store wants to send you targeted vouchers in store based on your previous shopping habits. An example of the how the GDPR strengthens individual rights is shown by the new Facebook privacy settings, which now give consumers the ability to see how their data is processed, or to be forgotten completely. The right to be forgotten is a major challenge for IoT devices. Although the GDPR aims to harmonise data protection rules across the EU and European Economic Area (EEA), it is important to consider other regulations that may overrule it. For example, clinical trials data, which could be captured from wearable health monitors, must be retained for 20 years after completion of the study, according to the Medical Research Council (MRC) in the UK [36].

3.6 Conclusion

The Helsinki Privacy Experiment of 2012 used 10 volunteer homes to investigate the "Long-term Effects of Ubiquitous Surveillance in the Home" over a 6-month period [37]. Sensors were implemented to track network traffic, personal computers, smartphones, cameras and payment cards. Interestingly, they found that despite initial aversion to monitoring, people became accustomed to the lack of privacy. One participant said that once he had accidentally been seen naked by the camera, his threshold for privacy was lowered. Outside of the confines of the experiment,

societies are becoming normalised to the lack of privacy as the desire for convenience and exciting new technology outweighs the risks of lack of privacy. Companies should take accountability for educating consumers on the rights they have on their personal data, and all corporations should be transparent about the way they process personal data, whether they are under control of the GDPR or not. Valuing the privacy of individuals should be considered by organisations as a competitive advantage, as it increases the trust between consumers and corporations, and between citizens and governments.

In this age of surveillance capitalism where we are moving ever closer to a digital panopticon, there has been a gap in privacy regulation and technological innovation, which has led to regulators scrambling to keep up. Nevertheless, the uptake of IoT devices has been slower than expected and this gives regulators an opportunity to leapfrog and cement their standards before IoT devices are deployed in even greater numbers around the world.

One must look at both sides and not forget the advantages of collecting vast troves of data from IoT devices. Data can be used for good—from personalising an individual's user experience to managing crime and monitoring health and well-being, decreasing the strain on health providers. IoT providers will increasingly need to communicate the value consumers gain when providing data. Proportionality is essential in ensuring a balance between technological innovation and privacy, a fundamental human right. The rapidly changing environment in which we live requires individuals to take ownership of their privacy, championed by governments and organisations. With the blurring of lines between online and offline, humans and artificial intelligence, we must not lose sight of what makes us human.

References

1. Royal Society (2017) The Internet of Things: opportunities and threats. Conference report. https://royalsociety.org/~/media/events/2017/10/tof-iot/iot-conference%20report-final.pdf. Accessed 14 Apr 2018
2. Cadwalladr C, Graham-Harrison E (2018) Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 14 Apr 2018
3. Banisar D, Davies S. Privacy and human rights. An International Survey of Privacy Laws and Practice. http://gilc.org/privacy/survey/intro.html. Accessed 14 Apr 2018
4. Wakefield J (2005) Children spend six hours or more a day on screens. https://www.bbc.co.uk/news/technology-32067158. Accessed 20 May 2018
5. Potuck M (2017) Barclays: 35% of consumers intending to buy an iPhone going with X. https://9to5mac.com/2017/12/04/iphone-x-barclays/. Accessed 20 May 2018
6. Kalischko T (2018) Google Marketing Live 2018 – Age of Assistance. https://smarter-ecommerce.com/blog/en/adwords-automation/google-text-ads/google-marketing-live-2018/. Accessed 27 Oct 2018
7. Manyika J, Chui M, Bisson P, Woetzel J, Dobbs R, Bughin J, Aharon D (2015) Unlocking the potential of the Internet of Things. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world. Accessed 12 May 2018

8. Michel F (1977) Discipline and punish: the birth of the prison. Pantheon Books, New York. Print
9. Hern A (2018) Fitness tracking app Strava gives away location of secret US army bases. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. Accessed 27 May 2018
10. BBC (2017) NHS cyber-attack: GPs and hospitals hit by ransomware. https://www.bbc.co.uk/news/health-39899646. Accessed 14 Jul 2018
11. Vaas L (2018) 350,000 cardiac devices need a security patch. https://nakedsecurity.sophos.com/2018/05/04/half-a-million-pacemakers-need-a-security-patch/. Accessed 14 Jul 2018
12. US FDA (2018) Battery Performance alert and cybersecurity firmware updates for certain Abbott (formerly St. Jude Medical) implantable cardiac devices: FDA safety communication. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm. Accessed 14 Jul 2018
13. Hullinger J (2014) How activists fooled the internet with these convincing new Google nest products. https://www.fastcompany.com/3030418/how-activists-fooled-the-internet-with-these-convincing-new-google-nest-products. Accessed 14 Jul 2018
14. Frenkel S (2017) US intelligence officials: latest WikiLeaks drop "Worse Than Snowden" Docs. https://www.buzzfeed.com/sheerafrenkel/us-intelligence-officials-latest-wikileaks-drop-worse-than-s?utm_term=.al62x3vpJ#.we6e14YzE. Accessed 14 Jul 2018
15. Nguyen N (2017) If you have a smart TV, take a closer look at your privacy settings. https://www.cnbc.com/2017/03/09/if-you-have-a-smart-tv-take-a-closer-look-at-your-privacy-settings.html. Accessed 14 Jul 2018
16. Cellan-Jones R (2017) Office puts chips under staff's skin. https://www.bbc.co.uk/news/technology-31042477. Accessed 7 Jul 2018
17. Reel M (2016) Secret cameras record Baltimore's every move from above. https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/. Accessed 7 Jul 2018
18. Hemmadi M (2017) Google's Sidewalk Labs project in Toronto is already creating jobs—in New York. https://www.macleans.ca/news/canada/googles-sidewalk-labs-project-in-toronto-is-already-creating-jobs-in-new-york/. Accessed 7 Jul 2018
19. Powles J (2015) Internet of things: the greatest mass surveillance infrastructure ever? https://www.theguardian.com/technology/2015/jul/15/internet-of-things-mass-surveillance. Accessed 7 Jul 2018
20. The Economist (2016) Where the smart is. https://www.economist.com/business/2016/06/11/where-the-smart-is. Accessed 7 Jul 2018
21. Kim E (2016) Amazon's Echo and Alexa could add $11 billion in revenue by 2020. http://uk.businessinsider.com/amazon-echo-alexa-add-11-billion-in-revenue-by-2020-2016-9?r=US&IR=T. Accessed 7 Jul 2018
22. Horcher G (2018) Woman says her Amazon device recorded private conversation, sent it out to random contact. https://www.kiro7.com/news/local/woman-says-her-amazon-device-recorded-private-conversation-sent-it-out-to-random-contact/755507974. Accessed 28 Jul 2018
23. US Patent and Trademark Office (2018) http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=%2Fnetahtml%2FPTO%2Fsearch-bool.html&r=1&f=G&l=50&co1=AND&d=PG01&s1=amazon.AANM.&s2=conversational&OS=AANM/amazon+AND+conversational&RS=AANM/amazon+AND+conversational. Accessed 28 Jul 2018
24. i-Scoop (2018) The new EU ePrivacy regulation: what you need to know. https://www.i-scoop.eu/gdpr/eu-eprivacy-regulation/. Accessed 28 Jul 2018
25. Kobie N (2015) Nudge theory: when your smart gadgets nag you. https://www.theguardian.com/technology/2015/aug/07/nudge-theory-smart-gadgets-silicon-valley. Accessed 14 Jul 2018
26. Nesta (2017) School children use the Internet of Things to tackle mental health issues. https://www.nesta.org.uk/news/school-children-use-the-internet-of-things-to-tackle-mental-health-issues/. Accessed 28 Jul 2018

27. The Canadian Press (2018) Federal health agency to mine social media for study on suicide trends, risk factors. https://www.theglobeandmail.com/life/article-federal-health-agency-to-mine-social-media-for-study-on-suicide-trends/. Accessed 28 Jul 2018
28. Buranyi S (2017) Rise of the racist robots – how AI is learning all our worst impulses. https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses. Accessed 28 Jul 2018
29. Dearden L (2017) How technology is allowing police to predict where and when crime will happen. https://www.independent.co.uk/news/uk/home-news/police-big-data-technology-predict-crime-hotspot-mapping-rusi-report-research-minority-report-a7963706.html. Accessed 28 Jul 2018
30. Ball J, Borger J, Greenwald G (2013) Revealed: how US and UK spy agencies defeat internet privacy and security. https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Accessed 28 Jul 2018
31. Ackerman S, Thielman S (2016) US intelligence chief: we might use the internet of things to spy on you. https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper. Accessed 28 Jul 2018
32. Hern A, Belam M (2018) LA Times among US-based news sites blocking EU users due to GDPR. https://www.theguardian.com/technology/2018/may/25/gdpr-us-based-news-web-sites-eu-internet-users-la-times. Accessed 28 Jul 2018
33. Farber D (2018) Salesforce CEO Marc Benioff Calls for National Privacy Law. https://www.salesforce.com/company/news-press/stories/2018/5/051618/. Accessed 28 Jul 2018
34. Intersoft Consulting (2018) https://gdpr-info.eu/art-13-gdpr/. Accessed 28 Jul
35. The Royal Society (2017) [starting at 30:00] https://www.youtube.com/watch?v=C_QXOHX5xSA&list=PLg7f-TkW11iWmGlFJ9-IkIffIcwRt9s74&index=3&t=0s. Accessed 28 Jul 2018
36. Medical Research Council (2017) MRC Regulatory Support Centre: Retention framework for research data and records. https://mrc.ukri.org/documents/pdf/retention-framework-for-research-data-and-records/. Accessed 28 July
37. Oulasvirta A, Pihlajamaa A, Perkiö J, Ray D, Vähäkangas T, Hasu T, Vainio N, Myllymäki P (2012) Long-term effects of ubiquitous surveillance in the home. Proceedings of the 2012 ACM conference on ubiquitous computing. UbiComp' 12:41–50