Tomorrow's Privacy

Internet of Things: security and privacy implications

Marie-Helen Maras*

New technology has afforded users with the ability to check the status of their home security from their smartphones, to start their car with a mobile phone application, and to remotely open and close their garage door from anywhere in the world. These technologies are becoming part of what is known as the Internet of Things (IoT). In its most basic sense, the IoT refers to the connection of everyday objects (eg TVs, appliances, and exercise equipment) to the Internet. It enables the real-time monitoring and vast collection of data about property, people, plants, and animals.

First, smart homes and offices have become part of the IoT. Specifically, these smart homes and offices enable light switches, doors, windows, blinds, and temperature to be controlled remotely. For example, WeMo by Belkin permits users to control power (eg energy usage), home electronics and appliances, water, and WiFi from a smartphone.[1] HomeKit by Apple, another smart home product, facilitates the control of alarm systems, surveillance systems, lights, and doors, among other objects, via an IPhone or IPad.[2] Other available technologies allow users to control their homes and offices via wristbands. For instance, Reemo wristbands enable users to control media (eg phones, video games, stereos, and TVs), security (eg alarm and surveillance systems), climate (eg thermostats, fireplaces, smart fans, and in-floor heating), and power (eg outlets, switches, and dimmers) in their home, using arm gestures.[3] These types of devices make the real-time monitoring of property, and movements and activities of people within the home and office possible.

Second, wearable devices have been developed that can monitor individuals' activities and vital signs. Fitbit is a fitness device that tracks and engages in the real-time monitoring of a user's distance travelled, steps taken, stairs climbed, calories burned, and quality of sleep, 24 h a day.[4] Hexoskin is clothing that monitors breathing rates, heart rates, and even tracks sleeping patterns of a user.[5] Other wearable devices promise 'to track . . . newborn's sleeping habits, gathering data like whether babies are on their backs or stomachs, their breathing rates, skin temperature,. . .and even, in some cases, blood-oxygen levels and heart rates'.[6] These devices allow the real-time surveillance of people, the inner workings of their bodies, and individuals' movements and activities.

Third, plants, gardens, and agriculture have become part of the IoT. For example, Oso Technologies' PlantLink

Key Points

- The Internet of Things (IoT) creates new security risks that device manufacturers and application developers have not anticipated.
- The devices that have become part of the IoT enable the storage, analysis, monitoring, and sharing of vast quantities of data with other networked devices and users.
- Users' privacy is threatened because of their limited control and choice over the collection, retention, and distribution of their data.
- The risk of an inadequate legal framework regulating the IoT requires urgent action in legal analysis and may require new approaches in legislation.

* Associate Professor, John Jay College of Criminal Justice, Deputy Chair for Security, Department of Security, Fire, and Emergency Management, 445 W. 59th Street, North Hall, Room 3405, New York, NY 10019. Tel: +1 212-621-4168; Email: mmaras@jjay.cuny.edu. There is no conflict of interest to declare. No ethical approvals are needed for this research. This article was not based on research that was funded by an outside source.

1 Belkin 'Wemo: Home Automation' <http://www.belkin.com/us/Products/home-automation/c/wemo-home-automation/> accessed 7 February 2015.

2 Apple 'HomeKit' <https://developer.apple.com/homekit/> accessed 7 February 2015.

3 Reemo <http://www.getreemo.com/> accessed 7 February 2015.

4 Fitbit <https://www.fitbit.com/compare> accessed 7 February 2015.

5 Hexoskin <http://www.hexoskin.com/> accessed 7 February 2015.

6 M Wood, 'Baby Monitors for a Smart Nursery, but Parents Are Still Better' *New York Times*, 3 December 2014 <http://www.nytimes.com/2014/12/04/technology/personaltech/smart-nurseries-track-a-babys-sleep-or-lack-thereof.html> accessed 7 February 2015.

© The Author 2015. Published by Oxford University Press. All rights reserved. For Permissions, please email: journals.permissions@oup.com

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017

provides real-time monitoring of plant moisture, thereby providing users with the means to keep track of when their plants need water.[7] With respect to agriculture, OnFarm lets users engage in real-time monitoring of crops through data from sensors, weather, maps, and protection measures.[8]

Finally, animals have become part of the IoT. A Dutch company, Sparked, uses sensors in cattle to monitor and track their health and movements.[9] Pets are also monitored and tracked with IoT devices. For instance, Whistle has a device that monitors pets' health and activities. Additionally, Tagg, now purchased by Whistle, has a device that tracks the location of pets via Global Positioning System (GPS) and their activities. Therefore, like property, people, and plants, IoT devices permit the real-time monitoring of animals, their activities, and movements.

The IoT is thus an interconnected system where living and inanimate objects in the physical world and sensors within or attached to them are connected to the Internet via wireless and wired network connections. These items can be controlled and monitored remotely through applications, which have been developed to enable sensing, automation, and machine to machine (M2M) communications. The latter, M2M communications, enables devices to translate data according to context and make relevant, timely, and valuable decisions based on readings. The IoT, therefore, improves efficiency through M2M communications and by allowing users to monitor people, items, and places, among others, in real-time at lower costs from anywhere in the world with an Internet connection.

Devices Not Built with Security in Mind

IoT devices not only monitor the user or target but also collect and relay information about the user and target. In particular, the IoT gathers data and relays this information to connected devices, where such data are stored, processed, and can be read by a user from mobile devices such as smartphones or tablets. Accordingly, IoT devices have the capability to sense, obtain, analyse, monitor, and distribute data on a massive scale. These devices also increase the amount of data that are collected, processed, stored, and transferred between IoT devices. Even medical devices, such as radiological machines (eg X-ray machines), biomedical devices, drug infusion pumps, pharmacy dispensary robots,[10] heart defibrillators, pacemakers, and surgical and anaesthesia devices, among others, have become part of the IoT. These IoT connected devices were created to improve efficiency and quality of life, and provide everyday conveniences to the user.

Nevertheless, the convenience of these devices comes at a cost, namely security. In fact, most IoT devices were built without security in mind. Indeed, many of these devices have backdoors placed on them by manufacturers and hardcoded manufacturer passwords. Furthermore, the security and privacy standards for these devices have not been adequately identified. Ultimately, the rush to deploy IoT technology has outpaced the creation and implementation of security and privacy protections and standards for these devices.

Risks Associated with the IoT

The IoT creates a greater attack surface by forming more access points to the Internet that need to be securely monitored. The greater the attack surface, the more vulnerabilities that exist which can be exploited. Therefore, bringing new devices online in the home, office, or other areas creates a slew of new threat concerns. These new threats were identified by Europol in 2014: 'With more objects being connected to the Internet and the creation of new types of critical infrastructure, we can expect to see (more) targeted attacks on existing and emerging infrastructures, including new forms of blackmailing and extortion schemes (e.g., ransomware for smart cars or smart homes), data theft, physical injury and possible death, and new types of botnets'.[11]

Primarily, these new devices linking property, people, plants, and animals to the Internet are vulnerable to hackers. A hacker can gain unauthorized access to IoT devices due to their set-up; that is, because these devices are connected, Internet-enabled, and lack the necessary protective measures. Because of these vulnerabilities, personal information collected by IoT devices could be misused. Particularly, if a device collects and stores personal, medical and/or financial data, a hacker could steal this information to facilitate identity theft.[12]

7 A Gebhart, 'This simple sensor will give your plant a voice' *CNET*, 28 May 2014 <http://www.cnet.com/products/oso-technologies-plantlink/> accessed 7 February 2015.

8 OnFarm <http://www.onfarm.com/> accessed 7 February 2015.

9 D Evans, 'The Internet of Things How the Next Evolution of the Internet Is Changing Everything' CISCO White Paper, April 2011 <http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> accessed 7 February 2015.

10 B Filkinds, 'Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon' A SANS Analyst Whitepaper, February 2014, <http://pages.norse-corp.com/rs/norse/images/Norse-SANS-Healthcare-Cyberthreat-Report2014.pdf> accessed 7 February 2015.

11 Europol, 'The Internet Organized Crime Threat Assessment', European Cybercrime Centre (EC3), 2014, 62.

12 Identity theft occurs to when an individual assumes the identity of a target (or targets) by unlawfully obtaining and using their name, social security

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017

These vulnerabilities also afford perpetrators with the opportunity to compromise these devices. An IoT device that has been compromised can be used to launch a denial of service (DoS) attack[13] or can be utilized to spread malware (ie malicious software). Cases in point are medical devices. Medical device manufacturers do not consider hacking and malware in the design of their products even though such devices are increasingly becoming Internet-enabled. These devices can be remotely controlled and the settings of these devices can be remotely changed. These devices additionally contain backdoors that make them vulnerable to potentially life-threatening attacks in the event that changes are made to existing settings. Specifically, attackers who know the default passwords of the devices can exploit the backdoors and change critical settings or replace the authorized firmware altogether. Depending on the devices, these actions can cause serious illnesses, injuries, and even death. This illustrates that the security of these devices is paramount. In the USA, the Health Insurance Portability and Accountability Act of 1996 requires that medical devices and medical device applications have the appropriate safeguards in place to protect against cyberattacks and unauthorized access, deletion, alteration, or disclosure of data from these devices. Also, in the European Union, Article 10c of Directive 2007/47/EC (amending Directive 90/385/EEC and Directive 93/42/EEC)[14] holds that medical device manufacturers should not place on the market or put into service any medical device that may compromise the safety and health of patients; such devices, if found, should be withdrawn from the market or be prohibited or restricted from being placed on the market or put into service.

The IoT device or devices that lack the appropriate safeguards (eg antivirus and antispyware software, firewalls, and intrusion detection systems/intrusion protection systems) can place the entire IoT system at risk. Endpoints that are poorly protected thus become gateways for cyberattacks seeking to take these devices offline, modify their settings, or render them unusable for a period of time. Insufficient protection of IoT devices and the data collected, stored, and transferred by them can further result in data breaches whereby individuals' data are stolen or compromised. Accordingly, wireless access points, databases, and data-collecting features of IoT devices and applications should be protected against hacking and security breaches.

Securing the IoT

If security issues are widespread within an IoT device that has been identified as vulnerable, class action and product liability lawsuits could be brought against IoT device manufacturers by affected customers. Other IoT stakeholders (eg application developers) could be held liable too; this will be determined by the level, if any, of their responsibility for the event that gave rise to the harm or damage that was caused.[15] Moreover, in the USA, companies can be charged for unfair or deceptive practices that adversely impact consumer security and privacy under the Federal Trade Commission Act of 1914.[16] In December 2013, the US Federal Trade Commission brought its first enforcement action against TRENDnet for its IoT devices (ie surveillance cameras that were used for home and baby monitoring).[17] According to the US Federal Trade Commission, TRENDnet's 'practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. . . . The acts and practices of [the] respondent . . . constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)'.[18] In its enforcement action, the US Federal Trade Commission charged TRENDnet with lax security practices and misleading customers by claiming that their IoT devices were secure. In reality, these devices had faulty software, resulting in the exposure of the private lives of hundreds of consumers; specifically, a hacker exploited a flaw in the software and posted links to the live feeds of approximately 700 consumer cameras.[19]

This case and others like it demonstrate the need for IoT infrastructure to be resilient to cyberattacks. To prevent these attacks, access control systems should be implemented to ensure that only authorized users access devices. Strong authentication measures are also needed

number (SSN), bank account number or other identifying information to commit a crime. MH Maras, *Computer Forensics: Cybercriminals, Laws and Evidence* (2nd edn, Jones and Bartlett, Massachusetts, 2014) 153.

13 A DoS attack occurs when an individual bombards a network server with more requests than it can handle, and in so doing, overwhelms its resources, eventually causing the server to shut down. MH Maras, *Computer Forensics: Cybercriminals, Laws and Evidence* (2nd edn, Jones and Bartlett, Massachusetts, 2014) 7.

14 European Parliament and Council Directive 2007/47/EC amending Council Directive 90/385/EEC on the approximation of the laws of the Member States relating to active implantable medical devices, Council Directive 93/42/EEC concerning medical devices and Directive 98/8/EEC concerning the placing of biocidal products on the market [2007] OJ L247/21.

15 Liability is covered in Article 23 of Council Directive (EC) 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

16 15 U.S.C. §§41–58, as amended.

17 In the Matter of TRENDnet, Inc., FTC. File No. 122–3090 (Complaint).

18 Ibid, para 18–19.

19 Ibid, para. 10.

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017

to prevent access to IoT devices and data. In addition, security safeguards should be built into devices. Consider medical devices. Medical device manufacturers can prevent the tampering of their devices by removing backdoor accounts and requiring all firmware to be digitally signed. The default passwords and usernames on these and other IoT devices should be reset as well.

Moreover, active firewalls and the use of a comprehensive security system (eg antivirus and antispyware software, and intrusion detection systems/intrusion prevention systems) are needed to protect IoT devices and detect threats. One example of such software is Bitdefender. Bitdefender is currently promoting one of its products, the Bitdefender box, as being able to protect everyday objects connected to a home network from malicious software.[20] Furthermore, to protect IoT devices, common security practices and standards are needed. The same level of security, however, will not be required for each IoT device. 'Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested'.[21] In line with this reasoning, Article 17 of the EU Data Protection Directive (Directive 95/46/EC) dictates that the level of security chosen should be appropriate to the risks posed by the information collected, stored, and transferred.[22]

The IoT Threatens Users' Privacy

In the future, more and more devices will become part of the IoT. This is evident due to the increase in new technologies that are IoT-enabled.[23] Purportedly, there are billions of IoT devices;[24] each of which are designed to harvest, store, and communicate a wealth of data. These data can easily be used to provide real-time information about a person, his/her health and finances, locations, contacts, habits, behaviours, and activities. Besides revealing these types of personal information, these data may also be used to detect and reveal changes in individuals' routines and displays of unusual behaviour. Ultimately, IoT devices create an environment where information on every person can be stored, analysed, monitored, made available, and shared with other networked devices and potentially other users. Given that vast quantities of information about individuals are being collected, processed, stored, and exchanged between IoT devices, people, and companies, considerable opportunity exists to create a detailed account of the private lives of millions of users.

Privacy is an essential human right and is protected in domestic (eg UK Human Rights Act of 1998), regional (eg the European Convention on Human Rights and the American Convention on Human Rights) and international human rights instruments (eg the Universal Declaration on Human Rights and the International Covenant on Civil and Political Rights). An essential element of privacy is the right and ability to keep certain things secret.[25] IoT users may have difficulty 'keeping things secret' because the '[f]ull development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed'.[26] Another essential element of privacy is the right to control the information others have and can access about oneself.[27] Users may have difficulty controlling their information because communications and data exchange between IoT devices 'can be triggered automatically as well as by default, without the individual being aware of it'.[28] What is more, 'modern techniques related to data analysis and cross-matching may lend this data to secondary uses, whether related or not to the purpose assigned to the original processing. Third parties requesting access to data collected by

20 M Wood, 'At the International CES, the Internet of Things Hits Home' *New York Times*, 4 January 2015. <http://www.nytimes.com/2015/01/05/technology/international-ces-the-internet-of-things-hits-homes.html?_r=0> accessed 7 February 2015.

21 Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 33.

22 Council Directive (EC) 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

23 IoT has dominated multiple technology shows, such as Consumer Electronics Show and the International Consumer Electronics Show, over the last couple of years. K Peterson, '"Internet of things" all the rage at Consumer Electronics Show', *CBS News*, 7 January 2015 <http://www.cbsnews.com/news/internet-of-things-all-the-rage-at-consumer-electronics-show/> accessed 7 February 2015; M Wood, 'At the International CES, the Internet of Things Hits Home', *New York Times*, 4 January 2015 <http://www.nytimes.com/2015/01/05/technology/international-ces-the-internet-of-things-hits-homes.html?_r=0> accessed 7 February 2015.

24 D Evans, 'The Internet of Things How the Next Evolution of the Internet Is Changing Everything', CISCO White Paper, April 2011 <http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> accessed 7 February 2015.

25 M Janis, R Kay, and A Bradley, *European Human Rights Law: Text and Materials* (2nd edn, Oxford University Press, Oxford, 2000) 300.

26 Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 2014, 8, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 7 February 2015.

27 C Fried, *An Anatomy of Values* (Harvard University Press, Cambridge, MA, 1970) 141.

28 Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 2014, 6, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 7 February 2015.

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017

other parties may thus want to make use of this data for totally different purposes'.[29] For example, data collected from IoT devices could be used to make credit, insurance, or employment decisions.[30] This can be particularly problematic if the IoT harvested data are used without the users' knowledge and consent or when the accuracy of the data has not been established.[31] These existing limitations on users' control and choice over the collection, storage, and transfer of IoT data threaten users' privacy.

Protecting Privacy

The European Union has a comprehensive data protection law, Directive 95/46/EC.[32] Directive 95/46/EC and its transposition into EU Member States' law regulates the processing and transfer of personal data and provides consumers with remedies for unauthorized disclosure, access, and/or use of their personal data. In Canada, the Personal Information Protection and Electronic Documents Act of 2000 is the primary data protection and privacy law regulating organizations' acquisition, use, and disclosure of personal information during commercial activities.

Unlike the European Union and Canada, the USA does not have a predominant data protection law governing the private sector. It does, however, have a data protection law that governs the public sector; namely, the Privacy Act of 1974.[33] This law requires government agencies to safeguard personal data, restricts the sharing of this information, enables citizens to seek civil remedies, and provides criminal penalties for violations of this law. Conversely, for the private sector, at the federal level, a sectoral approach towards data protection and privacy is followed, with laws regulating the collection, use, and disclosure of certain forms of personal information, such as health data (ie Health Insurance Portability and Accountability Act of 1996) and financial data (ie the Financial Services Modernization Act of 1999).[34]

The application of these laws to IoT device manufacturers, application developers, and others involved in the IoT may be limited. In fact, the US Government Accountability Office identified that the applicability of the Financial Services Modernization Act of 1999 and the Fair Credit Reporting Act of 1970[35] to information resellers was limited.[36] Accordingly, remedies for data protection and privacy violations exist in certain targeted areas (eg unauthorized financial and health data access, use, or disclosure) but do not apply to all those who collect, transfer, disclose, or otherwise use the data in some way. This approach, however, does not effectively deal with the data protection and privacy issues that arise with the deployment and use of IoT devices. Even the US Federal Trade Commission acknowledged that existing sectoral legislation is not designed to deal with the data protection and privacy issues arising from the use of certain IoT devices and applications. Specifically, in January 2015, the US Federal Trade Commission stated that the Health Insurance Portability and Accountability Act (HIPAA) standards should be updated because some IoT consumer-facing medical devices that collect similar sensitive information as doctors' offices and insurance companies may not be covered by HIPAA.[37] This deficit in existing legislation demonstrates the need for changes in the existing legislative framework that can deal with the risks posed by the IoT.

To protect personal data, self-regulation on the part of consumers is advocated. Individuals should be able to control and choose which data are collected, who is collecting it, and when this is occurring. The IoT is basically a repository for every aspect of a person's life. At the very least, '[a]pplications should facilitate the exercise of data subject rights of access, modification and deletion of personal information collected by IoT devices'.[38] In addition, the consent users provide for the use of an IoT device and the data collected by the device 'must be informed and freely given. Users should not be economically penalized or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service'.[39] Presently, users may be penalized or denied access to important services for choosing not

29 Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 2014, 7, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 7 February 2015.

30 Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 15.

31 Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 16.

32 Council Directive (EC) 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

33 5 U.S.C. § 552a.

34 The Financial Services Modernization Act is also known as the Gramm-Leach-Bliley Act (15 U.S.C. §§6801–6827).

35 15 U.S.C. §§ 1681–1681(u).

36 US Government Accountability Office, 'Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data', GAO-06-674, 26 July 2006, <http://www.gao.gov/assets/260/250627.html> accessed 8 March 2015.

37 Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 52.

38 Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 2014, 21–24, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 7 February 2015.

39 Article 29 Data Protection Working Party 'Opinion 8/2014 on the on Recent Developments on the Internet of Things' 2014, 21–24, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf> accessed 7 February 2015.

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017

to 'opt in' or provide 'affirmative consent' to the collection of their data. In the US automotive industry, 'consumers who choose not to consent to data collection may be denied access to valuable vehicle features. For instance, consent to sharing geolocation information for marketing purposes may be the only way for a consumer to turn on the navigation feature' in their vehicles.[40]

To safeguard personal data, it should be stored only as needed and data that are no longer needed should be periodically deleted. Data minimization should also be practised;[41] that is, the data collected should be limited to only that which is necessary for the effective functioning of the device and the application. This not only reduces the harm associated with data breaches but also minimizes the risk that data will be used in a way that deviates from user expectations.[42] Indeed, with IoT data, there is a significant risk that mission (or function) creep may occur, where the information obtained from certain devices will then be used for a wider set of applications outside of the original stated purposes for data retention. The type of data to be collected and its subsequent use should be clearly delineated in IoT privacy policies. Users should review these policies carefully as they reveal what information is collected, retained, used, and potentially transmitted to third parties.

Overall, existing practices insufficiently deal with the security and privacy concerns raised by the IoT. Ideally, a universal set of privacy and security standards should be developed. A barrier to creating a universal set of privacy and security standards is countries' (and even companies') differing views on these issues. Additionally, general privacy standards will not be accepted in countries that do not accord privacy the same importance and/or that fail to grant it special status as a human right (eg China) as other countries (eg the UK). What is currently being practised is the implementation of domestic laws regulating these issues and a general push towards self-regulation of IoT manufacturers and businesses. Self-regulation, however, will not suffice.

Users' data are valuable;[43] as such, companies are more prone to collecting and sharing this information, than refraining from collecting it or deleting it after collection. This practice, however, may change if the lack of such privacy protections will inevitably adversely impact companies' earnings (eg users may desist from utilizing these technologies when their privacy is not adequately protected). In the end, self-regulation will not work as companies are interested in promoting their own interests and increasing their profits, instead of protecting users' privacy.

Conclusion

The IoT connects and shares information about inanimate and living objects. Everything from medical devices and household appliances are being connected and becoming part of the IoT. New and changing manifestations of vulnerability are present with the use of IoT and its pervasiveness in society.

The protection of IoT devices is a multifaceted and complex process. The existing risk of an inadequate legal framework requires urgent action in legal analysis and may require new approaches in legislation. To effectively deal with existing IoT vulnerabilities, it is recommended that a thorough analysis of the existing applicable legal framework is undertaken and that new elements are developed to address the risks related to IoT deployment, wherever needed.

doi:10.1093/idpl/ipv004
Advance Access Publication 7 April 2015

40 EJ Markey, 'Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk' Staff of United States Senator for Massachusetts, 12 February 2015, <http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf> accessed 8 March 2015.

41 "Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD . . . [Guidelines on the Protection of Privacy and Transborder Flows of Personal Data], the 2002 Asia-Pacific Economic Cooperation ('APEC') Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights". Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 34.

42 Federal Trade Commission Staff Report, 'Internet of Things: Privacy and Security in a Connected World', January 2015, 34–35.

43 For example, companies can sell personal information to other companies for a fee for use for marketing and obtaining new clients.

Downloaded from http://idpl.oxfordjournals.org/ by guest on January 4, 2017