**UNDER PEER REVIEW**
DRAFT PAPER – Please do not cite or distribute without contacting the author

Dear Reader,

Thank you for taking the time and effort to review this working paper. Any feedback is very welcome and appreciated.

Best,

Nóra

# A Port in the Data-Sharing Storm: The GDPR and the Internet of Things

## 1. Introduction

By 2020, the European Commission has predicted that between 50 to 100 billion of these devices will be connected to the Internet.[1] Hence, the phrase of the 'Internet of Things' ('IoT') brings to mind a vision of sophisticated machines and systems in a (not so) futuristic society. In this envisaged ecosystem, all things communicate to each other because they are both connected to the Internet and to each other through the same central devices, such as an Internet-enabled phone/watch or an Artificial Intelligent ('AI') assistant, the most popular currently being Google's 'Alexa' or Amazon's Echo. This data-driven future (and present) follows a long history of enhancing our quality of life with emerging technologies. Most recently, in the nineteenth century, machines learned to do (locomotive trains, the telephone); in the twentieth century, they learned to think (the Internet); and today, in the twenty-first century, they are learning to perceive and ultimately think for themselves (AI).[2] In other words, machines now actually sense and automatically respond, including thermostats that turn on autonomously through sensors responding to changes in room temperature due to someone's presence in a room. The increasing role of technology in our daily lives, homes, and cities also aligns with the ever-advancing innovation and complexity of these inventions. For instance, 74% of EU households had access to fixed broadband Internet in 2016 compared to 57% in 2010 and seven out of ten European Union ('EU') businesses used mobile broadband in 2016, a noteworthy rise from just 28% in 2010.[3]

At the same time, 72% of EU Internet users worry that that too much of their personal data is being shared online and that they have little control over what happens to this information.[4] This is perhaps unsurprising given the increased media

[1] European Commission: Cluster of European Research Projects on the Internet of Things, *Vision and Challenges for Realising the Internet of Things*, March 2010: <http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf> accessed 12 April 2018.
[2] Ibid.
[3] Eurostat's 2016 Survey on Internet access and use statistics: < http://ec.europa.eu/eurostat/cache/infographs/ict/bloc-1a.html> accessed 2 July 2018.
[4] T. Bos, 'Clouds of Things – A European Digital Single Market for Cloud Computing, Big Data and the Internet of Things', European Commission – DG Connect Software, Services, Cloud computing, 24 October 2015; High Level Group of Scientific Advisors, *Cybersecurity in the European Digital Single Market: Scientific Opinion 2/2017* (European Commission, 2017), 59.

attention to some high profile and major online privacy and security breaches of business (e.g. Target and Equifax, two major U.S. companies) and government departments, including hospitals (e.g. WannaCry and Notpetya outbreaks) worldwide.[5] In 2016, the world's largest (distributed denial of service) attack on the Internet came from compromised IoT devices and brought down major websites across Europe and the U.S., including Twitter, Netflix, *The Guardian* and CNN.[6] There have also been recent reports of household IoT devices such as locks, thermostats, lighting systems and cameras, being used to harass and control in situations of domestic violence.[7] Hence, given the major vulnerability for data breaches across the many connected IoT devices and systems, ensuring data privacy and security should be a key priority for all those involved in the emerging IoT.

This article examines what role the recent major upgrade of EU data protection law, the General Data Protection Regulation ('GDPR')[8], may play in addressing the data protection implications and challenges posed by the IoT.[9] More specifically, the analysis focuses on the extended and new responsibilities to be met by data controllers and processors.[10] For instance, the new accountability principle (which forms part of many provisions under the GDPR) requires that controllers and processors (although ultimate responsibility remains with controllers for this) *demonstrate* at every stage of the data processing cycle that the GDPR is not only being complied with but that the policies and safeguards adopted are '*effective'*.[11] In addition, the GDPR strengthens a number of existing data protection rights and also establishes new rights for IoT users which should be taken into account in the design and development of IoT devices and systems. Furthermore, IoT stakeholders should consequently be prepared for the 'heightened sense' that users will have gained of the GDPR since its entry into force.[12] This may result in IoT users being more proactive in exercising their data protection rights, e.g. withdrawing their consent, exercising

[5] EU Agency for Network and Information Security (ENISA), *Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends* (2018): <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017> accessed 2 July 2018.

[6] N. Woolfe, 'DDOS attack that disrupted internet was largest of its kind in history, experts say', *The Guardian*, 26 October 2016.

[7] N. Bowles, "Thermostats, Locks, and Lights: Digital Tools of Domestic Abuse", *New York Times*, 23 June 2018.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ 2016 L119/1 ('GDPR').

[9] Other EU laws relevant to IoT stakeholders that are beyond the scope of this article include the E-Privacy Directive (2002/58/EC), soon to be upgraded as the E-Privacy Regulation, and the EU Directive on Network and Security Directive (2016/1148) (NIS Directive). For an overview of the NIS Directive and its relevance to the IoT, see F. Frederix (European Commission Cyber Security Unit), "How do Policy and Regulatory Initiatives address the topic of IoT security?", *ETSI Security Week*, 14 June 2016.

[10] Alternatively, for measures that also consider the responsibilities of IoT customers as IoT stakeholders in terms of strengthening user empowerment and data control, EU policymakers are increasingly promoting the benefits of "Personal Information Management Systems" (PIMS) to authorise the sharing of (but to not sell) personal data, see e.g. European Data Protection Supervisor (EDPS), *EDPS Opinion on Personal Information Management Systems*, Opinion 9/2016. For an example of one such PIM, see A. Chaudhry et al, "Personal Data: Thinking Inside the Box" (2015): <https://www.repository.cam.ac.uk/handle/1810/248792> accessed 2 July 2018.

[11] See e.g. GDPR, art.5(2); art.25; recital 74.

[12] P. Carey with B. Treacy, *Data Protection* (4th edn, Oxford University Press, 2015), 203.

their new right to data portability, or being represented by a NGO as part of a large group legal challenge (otherwise referred to as a class action[13]).

In order to clearly assess the application and influence of the GDPR on this emerging and complex area of technology, the article begins by explaining the concept and operation of the IoT. It then sets out the opportunities and challenges that this potentially transformative technology could bring for our quality of life, privacy, data security, and civil liberties. Subsequently, consideration is given to what has been heralded by EU policymakers and regulators as 'game changing' reforms to EU data protection law under the GDPR. [14] As is discussed below, this new legal regime represents both an evolution and revolution of EU data protection law and came into effect on 25 May 2018. The focus of this analysis specifically concerns provisions from the GDPR of particular relevance to IoT stakeholders (namely, manufacturers, retailers, and providers of IoT products and systems). These include the introduction of changes to the existing roles and responsibilities of data controllers and processors within the IoT framework. Other GDPR requirements also of relevance to IoT stakeholders are provisions mandating enhanced transparency, further internal compliance assessments (especially data protection impact assessments), the principles of 'Data Protection by Design and by Default', and the data subject's right to data portability. Some guidance for IoT stakeholders is also provided within this section. Last but far from least, the expanded, harmonised, and biting powers of enforcement and sanctions granted to data protection authorities under the GDPR are also addressed. These new enforcement powers could have serious consequences for IoT stakeholders found to be responsible for data protection violations, particularly in terms of the large fines that could be imposed or orders to temporarily or permanently cease data processing. In conclusion, some reflections are given on the extent of the role of the GDPR as a port for enhancing compliance with EU data protection law in the data-sharing storm of the IoT.

## 2. The 'Internet of Things

### *2.1. What is the 'Internet of Things'?*

As our clothes[15], cars[16], offices[17], homes[18], and cities[19], become ever more 'smart' (Internet-enabled), there are those who envisage that the logical next step is to

[13] GDPR, art.80(1) states that the right for an NGO to seek compensation on behalf of a group of claimants will depend on whether that is permitted by the law of the relevant EU Member State.

[14] See e.g., 'Awareness campaign on new data protection rules launched', *RTE News*, 25 May 2017: <https://www.rte.ie/news/technology/2017/0525/877893-data-protection/> accessed 12 April 2018.

[15] H. Tsukayama, "How Google and Levi's smart jacket shows what's coming next for wearables", *The Washington Post*, 14 March 2017.

[16] J.W. Bryans, 'The Internet of Automotive Things' (2017) 2(2) *Journal of Cyber Policy* 185.

[17] M. Choi, W. Park and I. Lee, "Smart Office Energy-Saving Service Using Bluetooth Low Energy Beacons and Smart Plugs" (2015) *IEEE International Conference on Data Science and Data Intensive Systems* 247.

[18] C. O'Brien, "Six easy ways to turn your house into a smart home", *The Irish Times*, 23 February 2017. For example, IKEA have launched their smart lighting platform in the U.S.: <http://www.ikea.com/us/en/catalog/products/90353361/>.

[19] See e.g. United Nations Human Settlements Programme (UN-Habitat), *Urbanization and Development: Emerging Futures – World Cities Report 2016* (UN-Habitat, 2016); N. Ni Loideain, "Cape Town as a Smart and Safe City: Implications for Privacy and Data Protection" (2017) 4(1) *International Data Privacy Law* 314.

connect all of these devices and systems as doing so may enhance our quality of life[20] and ensure that society is governed in ways that are more democratic, sustainable, and open. For instance, such a data-drenched network could make it harder for an authoritarian regime to control devices attached to online networks in order 'to choke off information flows'.[21] On the other hand, 'liberation technologies' such as smartphones will also generate so much data that will inevitably be of increasing interest to governments and industry, thereby raising major implications for an individual's privacy and autonomy.[22] This brings us to the connected environment in question, otherwise known as the 'Internet of Things' ('IoT').

The EU's body of data protection authorities from each EU Member State, the European Data Protection Board ('EDPB') (previously the Article 29 Working Party)[23], define the IoT as 'an infrastructure in which billions of sensors embedded in common, everyday devices – 'things' as such, or things linked to other objects or individuals – are designed to record, process, store and transfer data and, as they are associated with unique identifiers, interact with other devices or systems using networking capabilities'.[24] Such 'things' could be physical entities that directly interface with the physical world. Other broader definitions, however, for the IoT also extend to the potential of anything, physical (including the user) or virtual (e.g. cloud computing software services), capable of interaction (data exchange).[25] A less technical description, provided in a recent report by the UN Rapporteur for Freedom of Expression on the role of the private sector in the digital age, focuses on the potential vast application of the IoT: 'the avalanche of connectedness … in which digital connection is enabled for all aspects of contemporary existence'.[26]

Hence, as one leading computer security expert aptly observes, the IoT could be more accurately described as 'Things on the Internet' given that this new system seeks to give machines the power to monitor and manipulate the physical world by moving 'the bulk of internet communication from human-human communication mediated by computers, to computer-computer communication mediated by humans.[27] One multi-stakeholder, and multi-sector, based definition proposes that the IoT has generally been portrayed to comprise seven descriptive attributes. These identified elements define the IoT as: socially embedded; remote controllable; networked devices for information sharing between people, processes, and objects; an ecosystem of personal data stakeholders, e.g. third parties; physical objects with digital presence; backend computational infrastructure, e.g. cloud, databases, servers; device to device/backend communication without direct human input.[28] This framing of the IoT is particularly useful in two ways. First, the definition shows how the operation of the IoT has developed to date. Secondly, it also indicates the current

[20] See e.g. E. Constance, 'The Internet of Things: Preparing for the Revolution' (2017) 2(2) *Journal of Cyber Policy* 152.
[21] P.N. Howard, *Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up* (Yale University Press, 2015), 121.
[22] Ibid, 256-257.
[23] GDPR, art.68-76; art.94(2).
[24] Art.29 Working Party, Opinion 8/2014, *Recent Developments on the Internet of Things* (WP 223).
[25] J. Singh et al, "Twenty security considerations for cloud supported Internet of Things" (2015) *Internet of Things Journal IEEE* 1, 3.
[26] UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/32/38 (2016), 7.
[27] R. Mortier, "Explainer: The Internet of Things", *The Conversation*, 2 August 2013.
[28] L. Urquhart et al, "Realising the right to data portability for the domestic Internet of things" (2017) 22(2) *Personal and Ubiquitous Computing* 317.

overlapping elements in a variety of interpretations by policymakers, engineers, consultants, regulators, and academics which have each provided their own definitions of the IoT.

In terms of implementation, the IoT is already (and increasingly) operating *in part* within many households and offices due to a number of factors. These include the increasing low costs involved in the computing power and the ease and access to cheap cloud storage (e.g. Amazon), existing Internet connectivity, and the interest of governments and industry in extracting information from the masses of personal data (and other data) ubiquitously collected from all of the systems and devices involved. One such example is the use of smart thermostats that can detect human presence and adjust the air temperature accordingly and locking systems that are biometrically triggered.[29] For the individual, the IoT is already a feature of many people's daily life through the use of so-called 'wearables'. These include watches and glasses which may have sensors, microphones, or cameras embedded within them to enhance their traditional functions, e.g. Google Glass.[30] Devices for the 'quantified self' are worn regularly (if not constantly) in order for individuals to record, and then measure, their daily activities, e.g. sleep trackers.[31] Insurance companies have responded to the increasing shift by the public towards 'life-logging'[32] their lifestyles and exercise habits on the Internet by developing policies that incentivise their customers to be tracked by monitoring the amount of exercise they undertake daily in return for lower premiums.[33]

It is important to note that the ultimate aim of the IoT is to connect all individual devices, platforms, apps, and sensors, in order to integrate potentially every technology on the basis that data collection from a range of different sources are capable of diverse potential application.[34] Hence, since the term was coined in 1999[35], the IoT continues to be underpinned by the driving vision that the more data, systems, and devices that are connected - the better. This 'onward march' of the IoT heralds an all-encompassing data-driven society where the collection, analysis, sharing, and retention of personal data by service providers, machines, and objects will be pervasive and ubiquitous, thereby normalizing 'sustained data gathering from any source possible'.[36] In other words, the full realisation of the IoT would best be described as a data-sharing storm.

***How does the IoT work?***

A key question for users setting up future IoT networks is how large that environment will be. In other words, will the *thing* that a user is putting on the Internet be required

[29] U.S. President's Council of Advisors on Science and Technology (PCAST), *Big Data and Privacy Report* (PCAST, 2014), 23.
[30] See e.g. N. Bilton, "Why Google Glass Broke", *New York Times,* 4 February 2015.
[31] Information Commissioner's Office (ICO), *Big Data, Artificial Intelligence, Machine Learning and Data Protection* (London: ICO, 2017), 66.
[32] European Network and Information Security Agency (ENISA), *Risks and benefits of emerging lifelogging applications* (ENISA, 2011).
[33] See e.g. Vitality Health Insurance: <https://www.vitalitygroup.com/the-vitality-difference/proven-results/> accessed 12 April 2018.
[34] Singh et al (n 25).
[35] K. Ashton, *How to Fly a Horse: The Secret History of Creation, Invention and Discovery* (Anchor, 2015); See also, N. Gershenfeld, *When Things Start to Think* (Henry Holt, 2000).
[36] M. Nettesheim, "The CJEU's Decision on the Data Retention Directive" in B. Hess and C.M. Mariottini (eds), *Protecting Privacy in Private International and Procedural Law and by Data Protection* (Routledge, 2015), ch.3, 63; A. Daly, *Private Power, Online Information Flows and EU Law* (Hart, 2016), 118.

to communicate with all other Internet-enabled devices in the world or be limited to talking to other devices in their home or office. If it is the former, many identifiers/addresses for these things/devices will be involved and this creates considerable scope for multiplying points of failure in terms of ensuring that the same levels of data security and data protection compliance exist across such a large network.

For instance, as critical national infrastructure becomes increasingly Internet-enabled, new risks will emerge such as the hacking of a smart meter, thereby allowing that particular home's power to be controlled remotely and creating the possibility for an attacker to cause a power surge by turning on many homes' devices at once.[37] Consequently, as is discussed in further detail below, compliance by all IoT stakeholders (manufacturers and retailers of the relevant devices, systems, software and related updates) with the new GDPR principles of 'Data Protection by Design' and 'Data Protection by Default' will be crucial to ensuring the security and privacy of users' personal data collected and shared by their IoT devices and environments.

Another key question for users will be how to identify the thing that is to be put on the Internet in order for the device to be tracked, provide data, and controlled. This could be done by attaching a barcode to the device and then scanning the device with an Internet-enabled reader, as is already used by retailers for stocktaking and the tracking of goods. Computer engineers and ceramic designers have also undertaken research on using visual codes that are aesthetically pleasing that can be made to fit in with the ordinary patterns of that environment using recognition technology, e.g. embedding codes into patterns of the tableware of a restaurant.[38] The past decade, however, has seen the growing use of automatic identification technologies such as Radio Frequency Identification (RFID), potentially enabling the early development of the IoT by providing users with the capacity to interact with Internet-enabled objects.

RFID technology has provided for the humble barcode to be embedded in the object itself and to be read using electromagnetic waves to communicate with 'RFID Tags', with the possibility of reading the unique identification numbers of the *RFID Tags* or other information stored in them. RFID Tags are generally small and can take many forms but are often composed of electronic memory that is readable, and perhaps writable, and antennae.[39] *RFID Readers* are used to read the information on RFID Tags. *RFID Applications* process information developed through the interaction of RFID Tags and RFID Readers. Such Applications may be operated by one or more *RFID Application Operators* and are supported by back end systems and networked communication infrastructures. Examples of commonly-used RFID applications include the retrieval of additional product information in retailers simply by touching a RFID-tagged object with a smartphone and the integration of RFID Readers into smartphones enabling contactless payments, e.g. Apple Pay.[40] Visual barcodes may also be more convenient for users in terms of accessibility and convenience.

As noted by the Article 29 Working Party (as it then was), if an *RFID Application Operator* makes determinations related to the collection/use of personal data, it could hold the role of a data controller, as defined in the GDPR (further discussion below), who alone, or jointly with others, determines the purposes and means of operating an

[37] G. Cohen, Provocation Paper, *Data Management and Use: Governance in the 21st Century* (British Academy and Royal Society Report, London, 2017), 17.
[38] R. Meese et al, "From codes to patterns: designing interactive decoration for tableware" *CHI 2013,* April 27–May 2, 2013, Paris, France, ACM 978-1-4503-1899-0/13/04.
[39] Art.29 WP, *Privacy and Data Protection Impact Framework for RFID Applications* (2011), 3.
[40] Ibid.

RFID Application which has implications for the affected users' personal information.[41] In its preamble (the regulation's non-binding explanations), the GDPR specifically refers to RFID technology and also warns of the possible threats for an EU user's rights to privacy and data protection posed by the capacity of IoT-reliant technology for profiling. The new law does so by highlighting that users 'may be associated with online identifiers providers by their devices ... such as *radio frequency identification tags* [that] may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used *to create profiles* of natural persons and identify them.'[42]

In practice, many IoT products and services will operate by maintaining an ongoing relationship with users where their personal data (generated through the usage and operation of IoT devices and systems) is collected, mined, and analysed by IoT stakeholders in order to provide users value-added and tailored services.[43] Readings from the motion, temperature or carbon dioxide sensors (product usage data) can be combined to draw inferences, develop comprehensive behavioural profiles and make predictions about users.[44] How the relationship and sharing of responsibilities between IoT users and IoT stakeholders will develop will be a significant factor in the future development of the IoT and its impact on data privacy.

As highlighted by international bodies such as the World Economic Forum (WEF)[45] and relevant literature[46], major policy debates continue worldwide over where the balance of control and agency should rest between the empowerment of IoT users, particularly with regard to their role in management of their data, and the appropriate level of responsibility to place on those processing the personal data extracted from the IoT (data controllers and processors). Within the context of IoT contracts, users are often considered as the weaker party given the 'take it or leave' format of the terms, consequently resulting in the user being locked in to the contract with a noteworthy power imbalance created between users and IoT stakeholders.[47] As discussed below, the approach of EU policymakers under the GDPR has sought to address this power imbalance in three ways. First, the GDPR seeks to do so by increasing user empowerment through new rights such as data portability. Secondly, more responsibilities have been placed on data controllers. These obligations include requiring controllers to make their overall data-processing chain and relationship with processors more transparent and accountable and making data breach notifications to users mandatory. Thirdly, and perhaps critically, the GDPR strengthens and expands the scope of enforcement powers and potential liability of controllers and processors in case of a violation.

---

[41] Ibid, 4.
[42] GDPR, recital 30 (emphasis added).
[43] Urquhart et al (n 28).
[44] Ibid.
[45] *World Economic Forum, Rethinking Personal Data: A New Lens for Strengthening Trust* (2014): <http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf>.
[46] A. Crabtree and R. Mortier, "Personal data, privacy and the Internet of Things" (2016) *Social Science Research Network Paper*: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874312> accessed 2 July 2018.
[47] G. Nota La Diega and I. Walden, "Contracting for the 'Internet of Things': Looking into the Nest" (2016) 7(2) *European Journal of Law and Technology*; J. Lindqvist, "New challenges to personal data processing agreements" (2018) 26 *International Journal of Law and Information Technology* 45. For a contrasting view, see S.R. Peppet, "*Freedom of Contract in an Augmented Reality"* (2012) 59 *UCLA Law Review* 676.

### *2.2. The potential benefits*

As highlighted by the European Alliance for the IoT Innovation (AIOTI)[48] and in a recent report launched by the New Zealand government that has established an alliance with industry to accelerate the national-wide adoption of IoT technologies, advocates of the IoT consider it to be a 'transformative' technology.[49] Hence, the scope of the promised economic and social benefits associated with the success of the IoT is significant and growing. The ambitious objectives of IoT-driven strategies range from public authorities using technologies to better understand, visualise, and examine municipal infrastructure that will lead to improved resource allocation, to ultimately ensuring a better quality of life for all individuals.[50] IoT technologies are therefore expected to play a major role in improving the management of transport, energy use, water services, education, employment, health, crime prevention, by making society more efficient, innovative, safe, sustainable[51], and inclusive.[52]

For example, through the combination of Big Data and the IoT, Transport for London (TfL) have processed the personal data of millions of transport users on a daily basis collected through ticketing systems (Oyster pre-paid travel cards), sensors, CCTV, and social media, to improve the overall public transport system. Specifically, these systems have enabled TfL to send customers personalized updates on travel routes/disruptions, derive maps of users' most common travel patterns, and to identify travel improvements, including adding a new exit and entrance at Hammersmith Tube station.[53] On a more individual level, the IoT could provide a quality of life of greater efficiency, convenience, and safety that could be revolutionary in its scope. An area of particular interest in this regard is health care where the integrating of personal health and lifestyle monitoring devices into general health care services could deliver numerous benefits.[54]

These possible advances could include the provision of a regular and detailed source of personal data to a patient's doctor for diagnosis and treatment which in turn could improve disease prevention, make the overall healthcare system more efficient, and save individuals and doctors the time of traditional office check-up appointments.[55] The wealth of datasets collected could also radically transform medical research, leading to the better treatment or even eradication of diseases, and

---

[48] AIOTI, *Working Group 4 – Policy Report*, 15 October 2015.

[49] Minister for Economic Development, Communications and Transport, *Building a Digital Nation Report* (Wellington: March, 2017).

[50] S. Barns et al, "Digital Infrastructures and Urban Governance" (2017) 35(1) *Urban Policy and Research* 20.

[51] See e.g. O. Keogh, "Ambisense designs low-cost instruments to monitor quality levels of gas and air", *The Irish Times*, 26 January 2015.

[52] C. Perera et al, "Sensing as a service model for smart cities supported by Internet of Things" (2014) 25(1) *Transactions on Emerging Telecommunications Technologies* 81; K. Finch and O. Tene, "Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town" (2014) 41(5) *Fordham Urban Law Journal* 1581.

[53] L. Alton, "Improved Public Transport for London, Thanks to Big Data and the Internet of Things", *The London Datastore* (open data-sharing portal created by the Greater London Authority), 9 June 2015, *available* at: < https://data.london.gov.uk/blog/improved-public-transport-for-london-thanks-to-big-data-and-the-internet-of-things/ >.

[54] J. Bacon et al, "Personal and social communication services for health and lifestyle monitoring" *Proc. 1st International Conference on Global Health Challenges (Global Health 2012),* Venice, Italy, 21-26 October 2012.

[55] Federal Trade Commission (FTC), *Internet of Things: Privacy and Security in a Connected World* (Washington DC: FTC Staff Report, 2015), 7.

could also serve to make patients more informed and engaged with their healthcare, leading to more efficient treatment and substantial financial savings for patients.[56] Patients who suffer from diseases like Alzheimers but wish to live at home could have this freedom and autonomy and also have their safety ensured by monitoring the usage of their home IoT devices. The latter information could then be used to pinpoint their location in case they go astray.[57] Within the connected home, individuals with other disabilities could be empowered by being able to rely on a single platform using just one device by which they could control all household devices using a single app. Recently-developed smart phones now have such apps that can be used to control smart home appliances.[58] With respect to the added safety and benefit of connected cars, visually-impaired individuals could be in a position to use their own cars as a mode of transportation.[59]

Successfully achieving these transformative benefits, however, is dependent on IoT stakeholders establishing and maintaining high levels of privacy and security through technical efficiency, legal due diligence[60], and trust. By extension, satisfying these requirements is essential if the IoT is to play an increasingly major role in assisting individuals to better manage their lives and societies whilst being secure in the knowledge that their data privacy and security are adequately protected. Otherwise, concerns regarding the accuracy or reliability of the measured data and inferences provided to users from IoT devices, such as consumer health-monitoring wearables, raise issues of trust and power asymmetry between individuals and IoT advocates. For instance in 2018, disappointment with a wearable's performance has led to a class action legal challenge in California against *Fitbit* where the complainants allege that the company misled consumers about the device's ability to track user heart rate.[61] User experience and independent research cited in the legal proceedings indicate that the real-time heart rate monitoring provided by the technology used by *Fitbit* ('PurePulse') is 'grossly inaccurate and frequently [fails] to record any heart rate at all'.[62] These findings of general unreliability and inaccuracy in consumer heart rate monitors have also been replicated in recent independent scholarship by academics in Europe who highlight that the accuracy of such IoT devices is only likely to be improved by fundamental changes in, and therefore major upgrades to, the sensor technology.[63]

Furthermore, major risks to the privacy and security, and, consequently, the health and safety, of individuals abound if the technical robustness and reliability of both of hardware and software of IoT devices cannot be provided in alignment with the rapid march towards the widespread adoption of the IoT.

---

[56] Ibid.
[57] R. Wacks, *Privacy* (2nd edn, Oxford University Press, 2015), 27.
[58] L. Kelion, "Samsung Galaxy S8 hides home button and gains Bixby AI", *BBC News*, 29 March 2017.
[59] FTC Report (n 55).
[60] The UN Guiding Principles on Business and Human Rights (2011), ch.II (A)(17), highlights that due diligence compliance enables the private sector to identify, prevent, mitigate, and account for how they address their adverse human rights impacts.
[61] *Kate McLellan et al v Fitbit Inc*., U.S. District Court, Northern District of California, Case No: 3:16-cv-00036-JD, 5 June 2018: <https://www.lieffcabraser.com/pdf/Fitbit-060518-Order-re-Motion-to-Dismiss.pdf>.
[62] Ibid.
[63] T. Collins et al, "Reliability Assessment of New and Updated Consumer-Grade Activity and Heart Rate Monitors" (2018), Working Paper: <https://www.researchgate.net/publication/325828687_Reliability_Assessment_of_New_and_Updated_Consumer-Grade_Activity_and_Heart_Rate_Monitors>.

### *2.3. Risks to privacy and (data) security*

Data protection and computer security experts have raised a number of concerns regarding the risks that the IoT poses to the protection of an individual's personal data, privacy, and security. First, as a result of non-compliance with data protection principles and safeguards, the IoT may open up an individual's private life to a broad range of unauthorised and unlawful surveillance.[64] One of the most unsettling examples of such non-compliance have been IoT-enabled toys designed for the purpose of recording and storing records of young children's conversations without any limitation on collection, use, or disclosure of this personal information.[65] In addition to unlawfully recording and monitoring children's conversations, toy manufacturers (e.g. Genesis Toys) have also been found to have disregarded basic security safeguards in order to make their products easier to use.

By failing to prevent any unauthorised Bluetooth pairing by phones of unauthorized parties with the dolls in question, strangers could easily and covertly eavesdrop on children's conversations making them vulnerable to a substantial risk of harm, e.g. kidnapping, assault.[66] In 2016, EU and U.S. privacy and consumer advocacy organisations made complaints to data protection authorities demanding that IoT-enabled toy manufacturers adopt GPDR-compliant practices of privacy by design, and by default, throughout their product design process.[67] The organisations also highlighted that the terms and conditions of the companies relevant privacy policies warranted revision in order to clearly identify in future the user's data protection rights, provisions concerning data retention, and the purposes for which the data may be processed.[68] Another more infamous example of non-compliance by IoT stakeholders is the consistently weak security of Internet-connected baby monitors. These vulnerable systems have allowed hackers to remotely control the monitor's settings, view the camera footage, and to post online live feeds displaying babies while asleep and young children playing.[69]

Secondly, there is considerable concern that the unwieldy and complex interaction of different and multiple systems that all form part of the IoT will be unmanageable for users in practice. This will consequently challenge their ability to exercise any meaningful control over their privacy, data protection rights, and civil liberties generally. The Article 29 Working Party (as they then were[70]) rightly highlights that the constant interaction between objects, individuals and their devices, other individuals and their devices, and other systems will produce a generation of data

---

[64] Art. 29 Working Party, *Opinion 8/2014* (n 24).

[65] See e.g. Norwegian Consumer Council (NCC), *#Toyfail: An analysis of consumer and privacy issues in three internet-connected toys* (Oslo: NCC, 2016).

[66] Complaint to FTC, *In the Matter of Genesis Toys and Nuance Communications* (submitted by EPIC, Campaign for a Commercial Free Childhood, Center for Digital Democracy, Consumers Union), 6 December 2016, 20: <https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf >.

[67] Ibid; European Consumer Organisation (BEUC), "Consumer organisations across the EU take action against flawed internet-connected toys", Press Release, 6 December 2016:< http://www.beuc.eu/publications/consumer-organisations-across-eu-take-action-against-flawed-internet-connected-toys/html>.

[68] NCC Report (n 65).

[69] FTC, "Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy", *FTC Press Release*, 4 September 2013: <https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles>; D. Goodin, "9 baby monitors wide open to hacks that expose users' most private moments", *Ars Technica*, 9 February 2015.

[70] GDPR, art. 94: the EDPB replaced the Art.29 Working Party on 25 May 2018.

flows that 'can hardly be managed' with the traditional tools that are used to ensure the protection of individual's data protection interests and rights.[71] In the absence of being able to define virtual boundaries, by defining active or non-active zones for specific things, individuals may be unaware when devices/systems are communicating with each other. Consequently, individuals are then in an even more difficult position to control the subsequent use of the data by third parties, thereby enabling potential function creep.[72] Furthermore, this pervasive data-sharing environment, and threat of function creep, raise questions of the inevitable threat these potential developments pose for effective compliance with one of the core data protection principles - data minimisation.[73]

Accordingly, there are broader concerns that societies based on ubiquitous monitoring and surveillance mark the beginning of a trend of encroachment on an individual's private life, autonomy, and liberty, even if technologies are being employed in the interest of an individual, e.g. improving their health and safety.[74] The aggregation of personal data collected and retained by different IoT devices also fosters a culture of profiling. Strictly speaking, it could be argued that aggregation is merely the gathering of information about an individual. However, its overall effect could be unexpectedly intrusive given that the combining of innocuous pieces of information can reveal to the State or the private sector 'new facts', or inferences in the case of 'Big Data' used in AI-driven data analysis[75], about an individual, that could not be expected to be revealed, when the original isolated data was collected.[76] This data could then be used to identify an individual's personal and professional relationships, their racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership or data concerning health or sex life. Increasing the possibilities for profiling may also lead to the creation, or reinforcement, of unequal treatment in society.

It is these insidious threats of computer-enhanced discrimination and manipulation (e.g. through algorithmic decision making) that ought to raise considerable concern. Groups that face exclusion from access to goods, services or opportunities based on data obtained from their Internet usage, in this case via the IoT, are less likely to be aware of their status 'as victims of categorical discrimination'.[77] Hence, citizens could become increasingly unaware that their choices and behaviour are being constantly and systemically 'nudged', 'not only by states and governmental institutions, but also

[71] Art.29 Working Party, Opinion 8/2014 (n 24), 6.
[72] Ibid.
[73] GDPR, art.5.
[74] L. Taylor et al, *Customers, users or citizens? Inclusion, spatial data and governance in the smart city* (University of Amsterdam: Maps4Society Final Project Report, 2016), 14; B. Van der Sloot, "Do groups have a right to protect their group interest in privacy and should they?" in L. Floridi et al (eds.), *Group Privacy: New Challenges of Data Technologies* (Springer, 2017), ch.11, 271-272; Wacks (n 57), 28.
[75] Anton Vedder, "KDD: The Challenge to Individualism" (1999) 1 *Ethics & Information Technology* 275, 277; I. Rubinstein, "Big Data" (2013) 3(2) *International Data Privacy Law* 74, 78; D.K. Citron and F. Pasquale, "The scored society: Due process for automated predictions" (2014) 89(1) *Washington Law Review* 1; M. Hildebrandt, "Learning as a Machine: Crossovers Between Humans and Machines" (2017) 4(1) *Journal of Learning Analytics* 6, 16.
[76] D.J. Solove, *Understanding Privacy* (Harvard University Press, 2008), 118.
[77] O.H. Gandy, "Data Mining and Surveillance Post 9/11" in K. Ball and F. Webster (eds.), *Intensification of Surveillance* (London: Pluto, 2003), 37; L. Lessig, *Code and Other Laws of Cyberspace* (Basic Books, 1999), 153-154.

by businesses and perhaps in the future even by fellow citizens'.[78] Individuals may also be unfairly discriminated against because of how they have been placed in certain categories of groups based on characteristics/factors that their 'nearest neighbours' may have had although they may not in fact have any of these characteristics. This is because the AI system in question may have generated a non-distributive profile for them.[79] In practice, this may mean that an individual who lives in a certain neighbourhood where many people have a high healthcare risk may be denied health insurance, or charged a very high premium, even though they have always had a clean bill of health.[80] Consequently, individuals will be even less likely to seek redress by organising as an aggrieved group, or seek individual redress, 'in order to challenge their exclusion from opportunities in the market place, or in the public sphere'.[81]

Thirdly, the individual's privacy, security and safety may be compromised due to the lax implementation, or complete absence, of adequate data security standards, particularly because creating a more openly connected system of so many devices and systems increases the level of security risk. Accordingly, due to the pervasive use of wireless in local environments such as the home, the question of wireless security is increasing in urgency with the rise of the IoT.[82] Furthermore, as the number of connected devices increases and become an increasingly integrated part of daily life, the associated risks to privacy, data security, and personal safety are also likely to rise, particularly if these devices and systems 'lack the necessary protective measures'.[83] Invariably, the more devices and systems are connected to wireless networks in order to interact with the retailer, or to share information with other Internet network points (or nodes), the likelihood of hacking or illicit intercepting of sensitive personal data by third parties increases.[84]

As was stressed in a high level expert group report by the European Commission, the 'IoT is an enormous vulnerability when it comes to security and privacy protection' as each connected device or thing provides an easy first entry for hackers to reach more central systems.[85] Consequently, there are those in the cybersecurity community who (quite rightly) urge that no device should be connected to Internet if there is no way to update its vulnerability level.[86] The FBI has also called on the public to ensure that their IoT devices are 'isolated' from other network connections in order to lessen the risk of hacking.[87]These calls are most likely a response to the irresponsible business practice over the past decade by IoT stakeholders who launch their products on the market as cheaply and as quickly as possible, thereby leaving the data security of the user (and their trust of the IoT ecosystem as a whole) as an afterthought.[88] Ensuring that all IoT devices are by default switched on to include a

[78] Van der Sloot (n 74); R.H. Thaler and C. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness* (Yale University Press, 2008).
[79] Vedder (n 75).
[80] Ibid.
[81] Gandy (n 77).
[82] W. Schulz and J. van Hoboken, *Human Rights and Encryption: UNESCO Series on Internet Freedom* (Paris: UNESCO, 2016), 13.
[83] See e.g. M. Maras, "Internet of Things: security and privacy implications" (2015) 5 (2) *International Data Privacy Law* 99, 100.
[84] M.J. Cronin, *Smart Products, Smarter Services* (Cambridge University Press, 2010), 287.
[85] European Commission, *Cybersecurity Report* 2017 (n 4), 75.
[86] Ibid.
[87] U.S. Federal Bureau of Investigation Public Service Announcement, "Cyber Actors use Internet of Things Devices as Proxies for Anonymity and Pursuit of Malicious Cyber Activities", 2 August 2018: <https://www.ic3.gov/media/2018/180802.aspx> accessed 6 August 2018.
[88] Cronin (n 84), 306.

built-in and 'protected mode' of security falls exactly in line with the GDPR security obligations of IoT stakeholders, particularly the new data protection by design and default principles.[89]

Additionally, the IoT not only involves the processing of personal data through the use of billions of sensors, but also operates through 'actuators' which provide real-time data. For instance, the successful deployment of connected cars will rely on both sensors and actuators, which means that the IoT's impact on the 'physical world may result in greater risks for personal safety'.[90] A two-year research project on smart car security has already established that hacking a connected vehicle can be done wirelessly, with the hackers being able to take control of all of the car's internal computer systems, including the dashboard display, door locks, and brakes.[91] Perhaps unsurprisingly, as a result of the IoT becoming more widely adopted by governments, business, and individuals, Europol has warned that it expects to see hacks that will cause physical harm and possibly death, more targeted attacks on critical infrastructure, data/identity theft, new types of botnets, and the use of 'ransomware' on smart cars and smart homes for blackmail and extortion.[92] Ransomware is malicious software involving the 'use of device encryption attacks that encrypt the device of a user with a key that is kept by the attacker and only revealed in exchange for a ransom'.[93]

Major data security concerns have also been raised with respect to 'cloud'-supported IoT. Cloud computing ('the cloud') essentially consists of the concentration of resources, e.g. hardware and software, into a few physical locations by a cloud service provider (e.g. Amazon Web Service). The provider then offers 'those resources as services to a large number of consumers who are located in many different geographical locations around the globe over the Internet in an efficient manner'.[94] The three major service models from cloud computing involve the provision of infrastructure, platform, and software and have been a successful 21st century trend due to their resource effectiveness, notably cost and the convenience of outsourcing maintenance tasks such as backup and disaster recovery. The cloud has been described as the 'ideal component' for achieving the open sharing aim of the IoT framework as cloud services can operate across a range of systems and devices.[95]

This in turn provides a useful location for aggregating and examining the considerable amount of data to be collected by the IoT, in addition to the management and coordination of the many systems and services, it is always operating, and can scale to meet demand and resource constraints, e.g. battery, storage capacity.[96] Nevertheless, computer security experts have identified no less than twenty security-related considerations that raise a broad range of concerns over the IoT and the cloud. These concerns arise from the scale of the IoT, issues associated with identity management, issues of data management within the cloud and data transport to and from cloud services, issues arising from malicious 'things', issues of how to demonstrate effective certification and regulatory compliance which is key to user

[89] GDPR, art.5; art.25; art.32.
[90] Nota La Diega and Walden, (n 47).
[91] E. Naone, "Taking Control of Cars from Afar", *MIT Technology Review*, 14 March 2011.
[92] Europol, *The Internet Organized Crime Threat Assessment* (European Cybercrime Centre (EC3), 2014), para 4.4.2: < https://www.europol.europa.eu/iocta/2014/chap-4-4-2-view3.html >.
[93] UNESCO (n 82).
[94] Perera et al (n 52).
[95] Singh et al (n 25).
[96] Ibid.

trust, and issues arising from further decentralization into multiple clouds.[97] While the authors of this critical report accept that the IoT can yield many benefits, they highlight the crucial conflict of the former with that of the fundamental core element inherent in cloud services, which were 'designed with *protection* (isolation) as the dominant concern, with far less consideration given to *sharing*'.[98]

Resolving the above legal and technological issues is a challenge that should warrant concern from IoT stakeholders. There are those who argue that these hurdles, while major and inherently complex, can be overcome. IoT stakeholders will have to carefully evaluate how and where their compliance with the GDPR can be improved. This is will be no easy change for many IoT businesses (as discussed above) who have not given any prior consideration to potential security vulnerabilities in their hardware or software, thereby not making data protection law a priority to date. In order to do so, IoT stakeholders will have to undertake to meaningfully (re)design and develop the current IoT framework in order to ensure high security standards, including appropriate access controls that reflect the properties of the data (e.g. stricter access rules for sensitive data), anonymisation techniques, and enhanced transparency features.[99] Acknowledging the feasibility of this move towards greater due diligence and ultimately GDPR compliance, European Commission representatives have stated that the successful application of the IoT in this regard represents 'a technical challenge' and not the 'sacrificing of liberty, privacy and data security'.[100] As will now be discussed, although IoT stakeholders face considerable compliance hurdles, much of the success of effective GDPR implementation in the IoT will depend on the clarity and detail provided in the guidance of the EDPB's guidelines and opinions and on the enforcement approach of the DPAs.

## 3. The EU General Data Protection Regulation

### *3.1. A 'Game-Changing' Framework: An Overview for the IoT*

The GDPR has been described as no less than a potential 'Copernican Revolution' and 'game changer' in its reform of EU data protection law[101] and also places an enhanced emphasis on the principle of accountability and the risk-based approach. Data controllers were already required to ensure compliance under art.6(2) of the EU Data Protection Directive (95/46/EC), but the GDPR requires a much more proactive set of measures be undertaken by controllers in order to *explicitly demonstrate* GDPR compliance. This shift towards a more co-regulatory system of governance means more responsibility for controllers.[102] In particular, controllers now have to play a greater role in the overall oversight of their personal data processing within the IoT

[97] Ibid.
[98] Ibid.
[99] Finch and Tene (n 52); Singh et al (n 25).
[100] F. Frederix (DG Communications Networks, Content and Technology), "Smart Cars, Data Protection, and Encryption", 24 May 2016, *Technology and Democracy Project Workshop Seminar*, Centre for Research in the Arts, Social Sciences, and Humanities, University of Cambridge.
[101] C. Kuner, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law" (2012) *Bloomberg BNA Privacy and Security Law Report* 1: <https://ssrn.com/abstract=2162781>; ICO Commissioner, "The Role of Accountability in the GDPR", Lecture for the Institute of Chartered Accountants in England and Wales, London, 17 January 2017: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/01/gdpr-and-accountability/> last accessed 2 July 2018.
[102] For a detailed examination of Internet co-regulation and EU policymaking, see C.T. Marsden, *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace* (Cambridge University Press, 2011).

and other IoT stakeholders who process data on their behalf (processors and sub-processors). For instance, given the significant amounts of personal data increasingly collected, shared, and combined, by IoT devices and systems, the vulnerability of IoT users to security breaches, or other data protection violations, is an ongoing and inherent major risk that controllers must have under regular review. Controllers must also keep detailed records of any processing that poses a risk to IoT users and the technical (e.g. strong encryption) and organisational safeguards (e.g. adequate training for employees) in place to address such risks.[103]

Furthermore, controllers (and processors) should be mindful of the fact that the privacy and security risks will inevitably change, and most likely increase, given the new or extra IoT devices and systems that an individual, household, or organisation, is likely to add to their overall IoT ecosystem. Consequently, in the regular review of their 'Data Protection Impact Assessment' (DPIA)[104], one particular GDPR accountability-based requirement, controllers should be taking into account how often they are testing, verifying, and updating the vulnerabilities of the relevant hardware and software of their systems and devices. In its attempt to entrench the co-regulatory compliance culture that is key to the effective implementation of the GDPR, the Article 29 Working Party (as it then was) advises that it is best practice for controllers to treat a DPIA as part of their ongoing accountability obligations.[105] In the case of an audit or enforcement of sanctions following a major data breach, this means that data protection authorities will expect to see that this document have been 'continuously reviewed and regularly re-assessed'.[106] More than a decade earlier, as part of best practice, regulators made similar calls of companies that handle significant amounts of personal data, particularly sensitive data (e.g. health-related data), to undertake such assessments at least annually and to report to their stakeholders when they had done so.[107] Arguably, it is likely that data protection authorities will expect IoT controllers that process same to meet a similar deadline with respect to DPIAs.

Principally, the GDPR aims to move away from mere bureaucratic requirements, towards an updated framework for the 21st century that ensures meaningful compliance in practice and stronger data protection rights for individuals.[108] While it is welcome that the GDPR may indeed have an impact on the latter, it most certainly will not decrease the level of administrative burdens placed on controllers and processors. Given the added obligations and the wider adoption of the risk-based/co-regulatory approach which in turn places heavy emphasis on the new accountability principle that requires controllers to demonstrate compliance, it is likely that the GDPR will do just the opposite. This has led some commentators to aptly observe, within the context of the emerging IoT, that the GDPR will 'test the argument' of whether increased regulatory burdens may serve to stifle or encourage innovation

[103] GDPR, art.24; art.30.
[104] GDPR, art. 35. These assessments are required if the processing of personal data is 'likely to result *in a high risk'* to the rights and freedoms of natural persons (this means any individual, not just the IoT user/owner) (emphasis added).
[105] Art. 29 WP, *Guidelines on Data Protection Impact Assessment (DPIA)* (Revised), WP 248 rev.01, 4 April 2017.
[106] Ibid.
[107] See e.g. R. Thomas (former DPA) and M. Walport, *Data Sharing Review Report* (London: Ministry of Justice, 2008), 55.
[108] Kuner (n 100); R. Jay, *Guide to the General Data Protection Regulation* (Sweet & Maxwell, 2017), 181.

within the EU.[109]

The long-term impact of the GDPR notwithstanding, a number of reforms under the GDPR are of immediate relevance to IoT stakeholders. Underpinning most of these changes is the aim to empower individuals (IoT users/data subjects) by providing them with more control over their data. Although the GDPR leaves many of the key broad concepts ('personal data', 'processing', 'data controller') and principles from the now repealed Data Protection Directive (95/46/EC)[110] largely unchanged, it also creates new provisions and enhances the stringency and transparency requirements of existing rights and obligations. Hence, the GDPR represents both a *revolution* and an *evolution* for IoT stakeholders and also imposes a significant increase in obligations for data controllers and data processors.[111] For instance, the GDPR has established a pan-EU legal requirement for notification of a personal data breach to data protection authorities and individuals.[112] Previously, the regulatory approach of EU countries diverged between those with domestic breach notification laws (e.g. Germany) and those who required it as best practice (e.g. UK).[113]

Crucially, this, and other EU-wide, changes are also the result of the new EU data protection law being a 'regulation' and not a 'directive'. A regulation is more harmonizing in its approach as it becomes part of national law automatically without the need for a separate domestic law, whereas a directive allows EU Member States greater flexibility and requires that its aims be implemented through national legislation.[114] That being said, the GDPR does not achieve a complete harmonisation of data protection law across the EU. There are a number of derogations and exceptions within the GDPR where national legal systems have had to adopt their own laws in order to clarify their own specific approaches. IoT stakeholders for example that sell IoT toys (which collect, monitor, and share usage data from children) will have to check what age of consent for children (13-16 years of age) has been adopted in the laws of the different Member States where they sell or target their products.[115] In terms of preparing for the new rights established by the updated EU data protection law framework, the right to data portability is especially pertinent for IoT stakeholders.[116] A variation of the right to access, although narrower in scope[117], this new right is intended to prevent lock-in by providing data subjects with the ability to not just obtain and reuse. The new right also requires controllers to facilitate the transmission of data provided by customers directly from one service provider to another, where technically feasible.[118]

Finally, the GDPR also strengthens and harmonises the investigatory and oversight

---

[109] G. Rosner and E. Kenneally, *Clearly Opaque: Privacy Risks of the Internet of Things (IoT Forum*, 2018), 46.
[110] GDPR, art.94.
[111] On the changing roles and responsibilities of data controllers and processors, see P. Blume, "Controller and processor: is there a risk of confusion?" (2013) 3(2) *International Data Privacy Law* 140.
[112] GDPR, art.33 and art.34.
[113] P. Carey with B. Treacy (n 12), 130.
[114] P. Craig and G. de Búrca, *EU Law: Text, Cases, and Materials* (5th edn, Oxford University Press, 2011), 105-106.
[115] GDPR, art.3; art.8.
[116] GDPR, art.20.
[117] GDPR, art.20: the right to data portability only applies where the processing was by automated means and the relevant lawful basis was based on consent or was necessary for the performance of a contract.
[118] GDPR, art.20; Art 29 WP, *Guidelines on the right to data portability* (Revised) (WP 242 rev.01), 4 October 2017, 5.

powers of data protection authorities, as well as permitting said authorities to issue temporary or permanent bans on data processing, or major administrative fines, for lack of GDPR compliance.[119] While much attention has been focused on the scope of the new administrative fines which range into the millions of euro, a temporary or definite ban on processing for a particular IoT stakeholder may have serious implications for many other controllers, processors, and third parties linked to the impugned IoT stakeholder within a number of IoT data-supply chains.

### 3.2. *The IoT and GDPR compliance*

*New transparency and notice requirements*

Both EU case law[120] and guidance from the Article 29 Working Party[121] (as it then was) stress the importance of transparency as it underpins the data subject's right to access to information which thereby enables the exercise of other core data protection rights such as the right to object to data processing or to withdraw consent. This is all the more important in the data-driven IoT environment where the 'profiling' of users is rife. Ensuring a meaningful level of transparency, openness, and legibility of how such processing operates, and its consequences for the individual, is essential in order to avoid sleepwalking into a 'black box society'[122] where users are disempowered, uniformed, and therefore unable to place their trust in any kind of data sharing that benefits the individual or wider society. Hence, the transparency and notice safeguards of the GDPR require that clear and accessible information must be provided to data subjects with respect to the relevant data processing at issue and the rights available to data subjects.

Although the specific concept of 'transparency' is not defined in the binding provisions of the GDPR, some guidance is provided in other relevant articles and in the recitals. In particular, recital 39 specifically states that 'the principle of transparency requires that any information and communication relating to the processing of ... personal data be easily accessible and easy to understand, and that clear and plain language be used'. Some concern has been expressed regarding how exact the information provided must be, especially with regard to explaining to users how particular automated decision-making systems (particularly algorithmic-driven) systems operate.[123] Others have convincingly argued that algorithmic accountability and transparency have the potential to be stronger under the GDPR than the preceding requirements of the EU Data Protection Directive (95/46/EC) due the deterrent effect of major fines and investigatory powers, new accountability mechanisms (e.g. DPIAs), data breach notifications, and transparency requirements that will have a high impact on business reputation.[124]

---

[119] GDPR, art.58 and art.83.

[120] See e.g. Case C-201/14 *Bara Case*, EU:C:2014:238, para 33; Opinion of AG Cruz Villalon, ECLI:EU:C:2015:461, para 74.

[121] Art.29 WP, *Guidelines on transparency under Regulation 2016/679* (Revised), (WP 260 rev.01), 11 April 2018, 5 (now the EDPB).

[122] On the challenges posed by a lack of transparency and accountability surrounding automated decision-making, see F. Pasquale, *The Black Box Society* (Harvard University Press, 2015).

[123] S. Wachter, B. Mittlestadt, and L. Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) *International Data Privacy Law* 76.

[124] M. Hildebrandt, *"The Dawn of a Critical Transparency Right for the Profiling Era"* in J Bus et al (eds), *Digital Enlightenment Yearbook* (IOS Press, 2012); Hildebrandt (n 75); A.D. Selbst and J.

Rather than being all encompassing, the stated aim of the GDPR's transparency provisions with respect to privacy notices is to provide the data subject/IoT user with 'a *meaningful overview* of the *intended processing'*.[125] The requirements become more prescriptive, however, in the case of automated decision-making, like profiling – a form of processing often used by IoT stakeholders to tailor future products and services to customers. In a departure from the 1995 Directive, the GDPR provides a definition for profiling as any type of automated processing of personal data that provides analysis and predictions of an individual's personal aspects, including 'performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements'.[126] In this instance, the transparency requirements must include informing IoT users that automated decision-making is being used, and to provide as a minimum, 'meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject'.[127] Subject to certain circumstances, certain IoT stakeholders may be prohibited from using targeted online advertising from AI-driven profiling techniques that may result in 'legal' or 'similarly significant effects' for an IoT user.[128] The particular latter term of 'similarly significant effects' has rightly warranted criticism for its ambiguity.[129] In response, the Article 29 Working Party (now the EDPB) has provided some useful clarification in its GPDR guidance, as it is mandated to do.[130] This guidance provides examples of what constitutes a significant effect similar to that of a legal effect. For instance, it is advised that automated decision-making processes that use knowledge of a particular individual's socio-economic circumstances to exploit their vulnerability, such as regularly targeting online advertisements to individuals in debt or likely to be experiencing financial trouble and then being made likely to incur further debt, are prohibited.[131]

The GDPR also requires data controllers to comply with some very particular requirements with respect to time periods and the format of the language to be used in transparency/privacy notices. In terms of timing, if the personal data has been collected directly from the IoT user, then information must be provided when the personal data is being obtained[132] or at the 'commencement phase of the processing cycle'.[133] If the personal data of the IoT user has been obtained indirectly, e.g. through a data broker or a publicly available source[134], then the information should be

---

Powles, "Meaningful information and the right to explanation" (2017) 7(1) *International Data Privacy Law* 233; G. Malgeiri and G. Comandé, "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation" (2017) 7(4) *International Data Privacy Law* 243; M.E. Kaminsky, "The Right to Explanation, Explained" (2018) *University of Colorado Law School Legal Studies Research Paper* (No.18-24).

[125] GDPR, art.12(7) (emphasis added). In line with the EU Data Protection Directive (95/46/EC), GDPR, art.4(2) provides a very broad definition for what constitutes 'processing' which covers any type of operation involving personal data, e.g. collection, retention, analysis, storage, sharing, deletion.

[126] GDPR, art.4(4). For further, see M. Hildebrandt and S. Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer, 2008).

[127] GDPR, art.13(2); art.14(2).

[128] GDPR, art.22.

[129]

[130]

[131]

[132] GDPR, art.13(1).

[133] Art.29 WP, (n 120), 2018, 14.

[134] Ibid, 15.

provided within a month 'at the latest' to the IoT user.[135] Article 12 of the GDPR also requires that this information must be communicated in a 'concise, transparent, intelligible and easily accessible form, using clear and plain language'. Accordingly, the Article 29 Working Party (as it then was) advises that the format and language must be as 'user-friendly' as possible.[136] In other words, privacy notices will have to be rewritten/written in future to be tailored to the specific user. Hence, if an IoT toothbrush (toothbrushes embedded with sensors to track and send brushing habits to dentists for check-ups) is specifically designed for children, then the privacy notice information must be written in a language that will be clear and accessible to a child.[137] IoT stakeholders should note that the GDPR provides specific safeguards for the personal data processing of children due to them being less aware of the relevant consequences and risks. This means that if a child is below a certain age (13-16)[138], IoT stakeholders will have to 'make reasonable efforts' to verify that consent has been given by the parent/individual responsible for the child in the case of a children's IoT toothbrush.[139]

It is clear that the transparency requirements mandated by the GDPR are far more prescriptive than similar provided for under the EU Data Protection Directive (95/46/EC). This shift represents a challenge for many IoT stakeholders, especially data controllers and manufacturers. These changes include requiring controllers to provide more detailed and tailored privacy notices and to respond to a data subject's request for information within one month of receipt of the request.[140] IoT stakeholders will also need to invest resources in developing easily accessible mechanisms by which IoT users will be easily able to find such information. The Article 29 Working Party (as it then was) has proposed a number of methods for complying with this key GDPR principle. These include broadcasting the relevant information to be provided on the device itself by using wireless connectivity, or that device manufacturers could provide a QR code which could, describe the type of sensors in question, the information the device captures, as well as the purposes of these data collections.[141]

While the logistical challenges to providing such information in a format that will be read by users within the context of IoT products such as wearables has been acknowledged by data protection authorities, it is nevertheless considered feasible, and therefore expected, that IoT controllers satisfy these requirements. Consequently, the recommendation of data protection authorities for those processing data from emerging technologies and systems, like the IoT, is to prioritise making these requirements actionable as early as possible. Specifically, they urge controllers not to delay and to 'consider at an early stage of development how this information will be provided, and to look at the relationship between usability and privacy by design'.[142] Given the emphasis placed on transparency being 'an integral element' of demonstrating accountability, data protection authorities are likely to place

[135] GDPR, art.14(3).
[136] Art.29 WP, Opinion 8/2014 (n 24), 22.
[137] GDPR, art.12(1).
[138] GDPR, art.8(1) provides that the age where verifying consent for data processing of a child's use of Internet-based products or services from their guardian is required will depend on the age set by the national law of a particular EU Member State.
[139] GDPR, art.8; recital 38.
[140] GDPR, art.12(3): Taking into account the complexity of the request, and the number of requests, an extension of up to two months may be permitted but the reason for the delay must be provided to the data subject within one month of the request's receipt.
[141] Art. 29 Working Party, *Opinion 8/2014* (n 24), 18.
[142] See e.g. ICO (n 31), 66.

considerable importance on compliance with these new GDPR provisions.[143]

*Security: a 'new' principle and procedural measures*

The GDPR has elevated the ensuring of data security, from requirement to one of the key data protection principles that must be applied when processing personal data, with the establishment of the 'integrity and confidentiality' principle.[144] That being said, while *a newly-established core principle* under the GDPR, article 17 of the EU Data Protection Directive (95/46/EC) had already required data controllers to ensure an appropriate level of security in line with the risks posed by the relevant data processing. Article 32 of the GDPR carries forward the same requirements made of controllers under the 1995 Directive but is much more prescriptive and also rightly places further responsibility on processors for ensuring appropriate levels of data security. As before, the GDPR requires that the processing of the personal data must be done in a manner that ensures appropriate security of said data, 'including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'. The GDPR now also makes explicit reference for both controllers *and processors* to implement and ensure the effectiveness of specific security technical standards, i.e. use of pseudonymisation and encryption of personal data.

The aim for data controllers and processors to establish a compliance culture of pro-active accountability can also be seen in the new requirement for both to implement measures that provide 'a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing'.

Ensuing the maintenance of effectives security measures, both technical and organizational, for IoT stakeholders is a major data protection concern given the scope for data breaches due to the large amounts of data involved (and often sensitive data), and the ubiquitous data sharing between so many controllers, processors, and third parties. They may find that obtaining (and crucially adhering to) an *approved* GDPR certification mechanism helpful in saving time in the development of such policies, record keeping[145], and keeping track of their review, updating, and auditing.[146] It should be noted, however, that a growing number of businesses are making spurious claims that they are in the position to provide GDPR-approved certifications. Hence, IoT stakeholders should verify that these certification bodies have been accredited by a national data protection authority as required under the GDPR.[147]

The rise in status for ensuring data security under the GDPR aligns with the leading case law of the EU's highest court[148] concerning the fundamental right to the

[143] Art. 29 Working Party, *'Opinion 3/2010 on the principle of accountability'* (WP 173), 13 July 2010, 14.
[144] GDPR, art.5(1)(f).
[145] GDPR, art.30. Note that GDPR, art.30(5) provides a derogation for controllers that are small to medium companies (fewer than 250 employees) for record keeping requirements under the GDPR unless the processing is high risk.
[146] GDPR, art.42.
[147] GDPR, art.43(1).
[148] The Grand Chamber of the Court of Justice of the EU (CJEU/Luxembourg Court).

protection of personal data, as guaranteed by Article 8 of the EU Charter of Fundamental Rights. Since 2012, the Grand Chamber of the Court of Justice of the EU (CJEU) has consistently made clear that ensuring the requirements of data protection and security is 'an essential component of the protection of individuals with regard to the processing of personal data'.[149] Making security one of the key data protection principles also shows EU data protection law adopting a necessary evolving approach. Recognition of the need to adapt to ever-more sophisticated technologies is essential if these legal principles are to reflect present-day conditions in the digital age of ubiquitous connectivity. This makes the interpretation and application of the law adequate and relevant to the rapidly emerging technology of the IoT where the risk for security breaches is rife.

Article 32 of the GDPR also provides specific examples of the technical and organisational measures data controllers and data processors operating within the IoT should adopt in order to provide an appropriate level of security. This non-exhaustive list includes the pseudonymisation and encryption of personal data, and the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, and to restore availability and access to personal data in a timely manner following a physical, or technical, incident. IoT stakeholders should also provide that there is a process for regularly testing, assessing, and evaluating the effectiveness of these measures for ensuring the security of the processing.

The updated provision continues to provide that a number of factors will be taken into account when assessing if the level of security that an IoT stakeholder has adopted was appropriate to the risks of varying likelihood and severity represented by the data processing to the rights to the data subject. These factors include consideration of what technical measures were available at the material time to the IoT stakeholder (namely, were the standards 'state of the art'), the costs of implementation, and the nature, scope, context, and purposes of the processing. In other words, this assessment is done on a case-by-case basis. For instance, when dealing with the specific context of the processing of personal data, the Article 29 Working Party has stressed that IoT stakeholders in particular need to consider not just the security of the relevant device but also the wider environment in which the device will be operating in, e.g. communication links, storage infrastructure, other inputs of the ecosystem.[150]

The major focus placed on data security by the Article 29 Working Party in its IoT guidance is unsurprising given the major risk for end-to-end security posed by the chain of devices, systems, and things that comprise the IoT. A number of seemingly unavoidable factors underpin these concerns. These include the scale of the number of components involved, their overall integration, and the fact that such a wide network of data sharing is being provided for by an uncoordinated set of stakeholders. This leads to a system that 'only guarantees the level of security provided by the weakest component'.[151] As a result, poorly secured access points can become 'a gateway for cyber-attacks' allowing hackers to remotely take a device offline, modify critical

[149] Case C-614/10, *Commission v Austria,* EU:C:2012:631, para 37; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECR I-238, para 39; Joined Cases C-203/15 and C-698/15, *Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson,* EU:C:2016:970, paras. 123-124.
[150] Art.29 Working Party, *Opinion 8/2014* (n 24), 9.
[151] Art.29 Working Party, *Opinion 8/2014* (n 24).

settings, render the device unusable for however long, or make the device/system vulnerable to future attacks, resulting in blackmail, identity theft, injury, or death.[152]

*Certain breaches of data protection – reporting now mandatory*

The GDPR now requires IoT controllers across the EU to report a certain type of breach to a data protection authority within at least 72 hours from first becoming aware of the breach or without undue delay.[153] The obligation is a qualified one in that the regulators need only be notified if the breach is likely to result in a risk to the rights and freedoms of 'natural persons'. This latter term is important to note as it expands the scope of likely risk to the rights or freedoms of *any individual*, not just the IoT user/customer. If there is no such risk, then controllers are not required to inform the data protection authority but they must still make a record of the breach, its effects, and the remedial measures taken to address said breach.[154] The GDPR recitals highlight that the need for documentation to show that there was no risk, and therefore no need to inform a data protection authority, aligns with the requirements of the GDPR accountability principle.[155] Notably, the GDPR explicitly places an obligation on processors to notify controllers of any breach 'without undue delay'.[156] This shift in allocating greater responsibility to the role of the processor is welcome. It is also particularly relevant within the IoT where a considerable amount (if not the bulk) of much personal data processing is outsourced to processors, especially cloud service providers.[157]

For informing a data subject of a breach, the requirements are effectively much less onerous if the controllers and processors have been effective in their overall implementation of the GDPR. This is a major incentive towards encouraging proactive GDPR compliance. While a data protection authority must be notified if the breach is likely to result in *a risk* is posed to the rights and freedoms of natural persons, a data controller is only required to inform a data subject if the breach is likely to result in a *high risk*.[158] Furthermore, no notification at all is required if the controller meets the following conditions. First, the controller implemented appropriate technical and organisational protection measures, such as encryption, and these measures were applied to the personal data involved in the data breach. Secondly, the controller has been proactive and has subsequently taken steps to ensure that the high risk posed 'is no longer likely to materialise'. Lastly, informing the affected individuals would have involved 'disproportionate effort' and the same information could be made available to them 'in an equally effective manner', e.g. public communication (i.e. a newspaper advertisement).[159]

The GDPR also has a far less prescriptive approach with respect to the timeline for communicating the breach with data subjects, unlike the notification deadline period

[152] Maras (n 83), 101.
[153] GDPR, art.33(1).
[154] GDPR, art.33(5).
[155] GDPR, recital 85.
[156] GDPR, art.33(2).
[157] Although some types of outsourcing clearly constitute processing by a processor under the GDPR, some commentators argue that there are certain common types of processing by cloud service providers (e.g. hosting personal data without knowledge of said data) which should not result in their classification as 'processors': W Kuan Hon, C Millard, I Walden, "Who is responsible for 'personal data' in Cloud Computing" – The cloud of unknowing, Part 2" (2012) 2(1) *International Data Privacy Law* 3.
[158] GDPR, art.34(1).
[159] GDPR, art.34(3).

for alerting data protection authorities. Instead, data controllers are required to notify data subjects 'without undue delay'.[160] The recitals provide some more detail and advise controllers to notify data subjects 'as soon as reasonably feasible' although this should be done 'in close cooperation' with the relevant data protection authority.[161] In the case of 'an immediate risk of damage' (for instance, the leaking of credit card details), the need to mitigate harm caused would warrant 'a prompt communication' whereas advising users to implement appropriate measures to counter similar breaches in future (e.g. changing passwords) may justify a less immediate communication to data subjects.

Cybersecurity and legal experts have welcomed the mandatory nature of these new GDPR requirements.[162] In particular, it is argued that recording such breaches is the first step towards learning from them and should therefore be regarded as an opportunity for IoT stakeholders to increase the safety of compromised systems.[163] Consequently, these requirements to report certain breaches to data protection authorities and IoT users should contribute towards the development of an entrenched data security culture of compliance. Breach notification is also another mechanism that makes the transparency principle of the GDPR actionable by informing and thereby empowering data subjects. This also serves to enhance trustworthiness between IoT users and IoT stakeholders. Studies have found that transparency about the use and *protection* of customers' personal data reinforces trust.[164] The more trusted a brand is, the more willing individuals are to share their data. For an emerging market like the IoT, building and sustaining this trustworthiness, especially around data security compliance which has already raised concerns for users, is crucial to its sustained development and growth.

The mandatory breach notification requirement is a noteworthy change for data controllers within the IoT where data security is a major challenge and ultimately a data controller's overall responsibility, even with the increased of responsibilities that processors have now been given under the GDPR. Consequently, the responses and protocols for the detection, countering (e.g. high standards of encryption, secure administrative access), and notification process protocols for said breaches should all be clearly mapped out in an IoT data controller's 'Data Protection Impact Assessment'. These assessments are required if the processing of personal data is 'likely to result in a high risk' to the rights and freedoms of natural persons, not just the IoT user/owner.[165] Curiously, the GDPR does not require processors to undertake such an assessment. This may lead to difficulties in allocating liability in the case of future breaches as processors with dominate market power, e.g. particularly cloud providers such as Google and Amazon (Lambda), have already adopted a practice of issuing instructions to controllers in contractual agreements.[166] In order to keep costs

[160] GDPR, art.34(1).
[161] GDPR, recital 86.
[162] Hildebrandt (n 75); Bryans (n 16); Y. Padova, "What the European Draft Regulation on Personal Data is going to change for companies" (2013) 4(1) *International Data Privacy Law* 39.
[163] Bryans (n 16), 194.
[164] See e.g. T. Morey et al, "Customer Data: Designing for Transparency and Trust", (2015) *Harvard Business Review* 96 (May issue): <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust> accessed 12 July 2018. The results from the 2015 international research study, which had 900 participants from the U.S., Germany, UK, China, India, showed that social media companies ranked as the least trustworthy with primary care doctors and credit card companies closely ranked as being the most trustworthy.
[165] GDPR, art.35.
[166] Lindqvist (n 47), 54.

down, IoT controllers are increasingly turning to cloud providers for much of their data storage and processing (e.g. use of cloud platforms to design apps that enable the collection of data from IoT devices), thereby outsourcing much of their institutional understanding of how these systems operate. This enables an environment where controllers are unable to be accountable for the data-supply chain and whereby processors may have 'an upper hand' and could process data for its own purposes.[167] Such a case arose in Sweden where the data protection authority found that a Swedish municipality (Salem) was using Google Apps Cloud services for its e-mail and calendar functions but did not have sufficient insight, detail, or control over the processing activities, or sub-processing activities of Google, in its agreements with Google.[168] Data protection authorities in Norway also raised similar concerns concerning the use Google Cloud Services by local authorities.[169]

Hence, data protection authorities (particularly the EDPB) also have a major role to play in the adequate enforcement and monitoring of the different responsibilities that should be allocated to those IoT stakeholders who make significant decision-making with regard to the processing of personal data. In other words, regulators should in future clearly highlight in their guidance, opinions, and recommendation, what factors IoT controllers should consider in identifying whether processors are in fact making decisions of such importance that they should actually be reclassified as having the role (and crucially the responsibilities and liabilities) of a 'joint controller'.

*The new right to data portability*

Article 20 of the GDPR establishes the new right of data portability and aims to empower individuals regarding the control of their data. Subject to certain conditions, the right facilitates an individual's ability to move, copy, or transmit personal data *concerning him or her* from one IT environment to another (such as the data subject's own possession, the system of a trusted third party or a new data controller). If an individual exercises this right, the personal data to be transmitted must be provided in 'a structured, commonly used and machine-readable format'. The application of this new GDPR right is limited, however, to certain types of 'personal data' and by the other key following circumstances, making it both an 'evolution' of, but much more narrow in scope than, the right of access under article 15 of the GDPR.[170]

First, the individual must have *provided* this personal data concerning them to the data controller.[171] Secondly, the legal basis of the data processing in question must have been the data subject's consent, or the processing was necessary for the performance of a contract. Thirdly, the processing must have been carried out by automatic means. In reducing the risks for the personal data of third parties that may be transmitted, the Article 29 Working Party encourages data controllers to implement tools that will enable data subjects to select the relevant data that they wish

[167] Ibid, 55.
[168] Ibid.
[169] L Tung, "No personal data on Google Apps, Norway tells its councils as it clears cloud use" *ZDNET*, 27 September 2017: <https://www.zdnet.com/article/no-personal-data-on-google-apps-norway-tells-its-councils-as-it-clears-cloud-use/> accessed 12 July 2018.
[170] P. Swire and Y. Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique" (2013) 72(2) *Maryland Law Review* 335; O. Lynskey, "Aligning data protection rights with competition law remedies? The GDPR right to data portability" (2017) 42(6) *European Law Review* 793; L. Scudiero, "Bringing your data everywhere: a legal reading of the right to data portability" (2017) 3(1) *European Data Protection Law Review* 119.
[171] GDPR, art.15.

to receive and to exclude, where relevant, the data of other individuals.[172] In order to ensure 'fair and transparent processing', Articles 13 and 14 of the GDPR require that data controllers must inform data subjects of their right to data portability at the time when their personal data is obtained, if directly collected, or within a month, if the data has not been obtained from the data subject. Finally, under article 12(5) of the GDPR, the right to data portability must be exercised, and free of charge, unless the data controller can show that the data subject's request is 'manifestly unfounded or excessive'.

The Article 29 Working Party contends that the primary aim of data portability is to enhance an individual's control over their personal data and to make sure "they play an active role in the data ecosystem".[173] Arguably, however, data portability does not amount to a significant empowerment of the data subject in practice as the effective exercise of consent, and its withdrawal at any time by him/her, could presumably bring about the same result (GDPR, article 7).[174] Nevertheless, the Working Party has interpreted the scope of the personal data "provided by" the data subject within the 'new' right to data portability broadly. A literal interpretation of personal data knowingly and actively provided by an individual to an IoT stakeholder would likely include account or subscription data, such the data subject's name, address, or other contact details. In contrast, the Working Party argue that personal data "provided by" the data subject also results from observing their activity/device usage.[175] Consequently, in order to give "full value" to the right of data portability, it is argued that this personal data thereby extends to the activities of users including raw data processed by connected objects (e.g. smart meters) such as activity logs, website usage, or search history. Critically for IoT stakeholders, the broad (and controversial[176]) interpretation of this scope does not, however, apply to any subsequent analysis of the data subject's behaviour (e.g. user profile) generated by data controllers from the IoT user's personal data.

While acknowledging the potential for data portability to counter the potential lock-in effect of certain (monopolist) IoT ecosystems, concerns have been raised with respect to the issues that this right could pose in practice if poorly implemented in practice. For instance, given the vast amount of data retained over years that could be involved in a data portability request (especially from IoT devices and systems), it will be crucial that data controllers ensure that the highest levels of security (esp. strong ID authentication) will apply to the transmission of what could be very sensitive private information in order to prevent a personal data breach.[177] Problems may also arise given the silence in the GDPR with respect to mandating a particular form of interoperability for different systems.[178] Recital 68 of the GDPR instead merely provides that data controllers 'should be encouraged' to develop interoperable formats that enable data portability. As a result, a key factor in the success of data portability within the IoT ecosystem will depend on the level of cooperation between IoT stakeholders working together to develop a common set of interoperable

[172] Article 29 Working Party (n 62), 2.
[173] Ibid.
[174] P. de Hert and V. Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" (2016) 32(2) *Computer Law and Security Review* 179.
[175] Article 29 Working Party (n 62).
[176] D. Meyer, "European Commission, experts uneasy about WP29 data portability interpretation": <https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/> accessed 2 July 2018.
[177] Swire and Lagos (n 170), 375.
[178] Daly (n 36), 116.

standards and formats. IT departments and employees of any IoT stakeholders, and the IT design community responsible for developing both such standards and formats within the IoT, therefore, have a considerable role to play in realising of the right to data portability and will need to be allocated the appropriate resources in order to effectively undertaken this task. [179]

*'New' principles of data protection by design and by default*

Article 25 of the GDPR establishes the principles of data protection by design and default, which are referred to interchangeably with the more widely known 'privacy by design' approach, drawn in turn from the development of the privacy-enhancing technology (PET) concept in the 1990s. [180] Essentially, these principles convey that privacy and data protection safeguards should be considered from the very beginning of a system's/device's development to the operation of the processing itself. Notably, article 14 of the 2002 e-Privacy Directive can be interpreted as already calling for a privacy-by-design approach given that it encourages Member States to establish rules on how to design terminal equipment in such a way that is compatible with the right of individuals to protect and control the use of their personal data.[181]

Under article 25, the data protection by design approach requires that data controllers implement "appropriate technical and organisational measures" (e.g. pseudonymisation), which are designed to effectively implement data protection principles (e.g. data minimisation), by integrating the necessary safeguards into the processing. Data controllers are expected to take into account a number of factors when implementing this approach, including the cost, the appropriate level of technical sophistication required given the nature, scope, context, purposes of the processing, and the risks posed to the data subject's rights by the processing. The data protection by default principle also obliges data controllers to implement a holistic approach (appropriate technical and organisational measures) for ensuring that personal data are only processed for a necessary specific purpose(s). This obligation covers the amount of personal data collected, the extent of their processing, storage period, and accessibility.

Within the IoT context, practical examples of demonstrating compliance with these principles would include undertaking a privacy impact assessment (PIA) before launching any new IoT applications and making the PIA publicly accessible (in full or in part).[182] Secondly, where only aggregated data is needed for processing, IoT stakeholders could arrange for the raw data collected by IoT devices to be deleted at the nearest point of collection, e.g. on the same device after processing.[183] Ensuring that data protection safeguards are built into the architecture of IoT systems will only increase in importance for preventing (what may be unintended) privacy violations and discrimination given the rise in automatic decision-making and data-driven

[179] Urquhart et al (n 28).
[180] P. Hustinx, "Privacy by design: Delivering the Promises", paper delivered at the Privacy by Design Workshop, 2009: < https://edps.europa.eu/sites/edp/files/publication/09-11-02_madrid_privacybydesign_en.pdf>; A. Cavoukian, "Privacy by design. The definitive workshop" (2010) 3(2) *Identity in the Information Society* 247.
[181] G. Danezis et al, *Privacy and Data Protection by Design – from policy to engineering* (ENISA, 2014), 55.
[182] For further, see A. Warren et al, "Privacy Impact Assessments: International experience as a basis for UK Guidance" (2008) 24 *Computer Law and Security Report* 233; Article 29 Working Party, Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, *available* at: <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf>.
[183] Art.29 Working Party, Opinion 8/2014 (n 24), 21.

software systems (algorithmic surveillance) that construct profiles of individuals from personal data shared out of context. As a result, if meaningfully implemented, data protection by design "could serve as an effective means to achieve 'technological due process'" within the sphere of learning analytics.[184] As a way of demonstrating compliance with these key principles, IoT stakeholders could apply for a certification mechanism, data protection seal or mark, subject to criteria approved by a national data protection authority or the European Data Protection Board (GDPR, article 42).

*Anonymisation of data - a means to avoid GDPR Compliance?*

The principles and requirements of the GDPR do not apply if an IoT stakeholder makes the personal data that is being collected from an IoT device anonymous. The GDPR defines the latter term as "information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable".[185] This could be regarded as a means by which to avoid GDPR compliance altogether but still allow manufacturers to extra value from IoT user data.

Caution, however, is urged against pursuing such an approach given the increasing amount of research published on the techniques that can extract identifiable information (personal data) from anonymised data.[186] In other words, these techniques allow for the *re-identification* of data. Furthermore, the correlation of shared data, in other words the IoT *modus operandi*, from (what is often many) IoT devices (and systems and networks) only increases this risk.[187] For instance, research has showed that individuals could be identified based on snippets of in-vehicle sensor data from their driving behaviour.[188] Increasingly, the dramatic and increasing rise of connected devices over the Internet and data sharing has put all data processing on a spectrum of risk. In line with the data protection by design and default principles of the GDPR[189], even with what is considered to be a robust form of anonymization, preventative measures and safeguards must now always now be taken to ensure against any breaches or misuse of data. Once re-identified, information falls back within the broad scope of "personal data", which is "any information" that either, directly or indirectly, identifies a person within the EU or makes them identifiable[190], and thereby any processing of said data by an IoT stakeholder will be subject to the application of the GDPR. Put another way, "as reidentification science advances, it expands the EU [GDPR] like an ideal gas to fit the shape of its container".[191]

Instead, a more useful approach for IoT stakeholders to consider would be complying with the GDPR and designing personal data collection and processing systems that comply with the long established data protection principle of data minimisation.[192] This could be done by ensuring the use of pseudonymisation

[184] Hildebrant, (n 75), 8.
[185] GDPR, recital 26.
[186] See e.g. P. Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 75 *UCLA Law Review* 1701.
[187] Bryans (n 16), 191.
[188] E. Miro et al, "Automobile Driver Fingerprinting" (2016) *Proceedings on Privacy Enhancing Technologies* 1, 34–50.
[189] GDPR, art.25.
[190] GDPR, art.4(1).
[191] Ohm (n XX), 1741.
[192] GDPR, art.5(1)(c) provides that personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.

(encryption of personal/identifiable data)[193] as much as possible throughout the data processing cycle. Within the IoT context, data minimisation in practice would involve minimising the processing (disclosure/sharing/storage/use) of personal data. In other words, in line with the GDPR principles of data protection by design and by default, IoT users should be able to access, or switch on, any of their IoT devices without having to provide "full identity disclosure".[194]

### *3.3. Failing GDPR compliance …*

IoT stakeholders should take particular note of the expanded powers to be granted to data protection authorities, especially with respect to enforcement, non-compliance, and sanctions, once the GDPR enters into force in May 2018.[195] For instance, with respect to their investigatory powers, data protection authorities (in line with EU and national laws) shall have the power to obtain "access to any premises of the controller and the processor, including to any data processing equipment and means". Under the wide-ranging scope of corrective powers, data protection authorities may order the withdrawal of certification (mechanisms/seals/marks indicating data protection compliance), or order the non-renewal of such by the relevant certification body, if the relevant standards are no longer being met.

Should the implementation of these certifications be the subject of effective mainstream implementation by the private sector, accompanied by meaningful standards and effective oversight by the European Data Protection Board, DPAs, and civil society, their removal should raise major concern for IoT users. Consequently, the exercise of such a corrective power could then represent a significant risk of reputational damage to the brand of the relevant data controller/data processor. By extension, such reputational damage would then have serious implications for the level of trust data subjects/customers will place in the privacy and security of these uncertified IoT systems and devices. This reputational damage could in turn result in an increase in litigation and class action lawsuits against data controllers who are not GDPR compliant (GDPR, article 80).

Without question, the administrative fines provided for in the GDPR are severe and give teeth to the law's new accountability principle. The latter requires that data controllers shall be responsible for, and be able to demonstrate compliance with, the basic data protection principles when processing personal data (GDPR, article 5). For IoT stakeholders, processing personal data without ensuring an appropriate level of security, allowing for unauthorised/unlawful processing of a user's personal data, or its accidental loss, destruction or damage, could thereby result in a major sanction. Under article 83(5) of the GDPR, data controllers could be subject to an administrative fines of up to 20, 000, 000 EUR, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. When imposing such a fine, national supervisory authorities are required to ensure that the sanction is effective, proportionate, and dissuasive.

The risk-based approach taken by the supervisory authorities when determining whether to impose a fine, and the scope of the amount involved, will take into account

[193] GDPR, recital 26, defines the process of pseudonymisation as: 'Personal data ... which could be attributed to a natural person by the use of additional information'. It is therefore still considered to fall within the meaning of personal data, thereby falling within the material scope of the GDPR.
[194] European Commission, *Cybersecurity Report* 2017 (n XX), 73.
[195] GDPR, art.58.

a number of factors. These circumstances will include the nature, gravity, and duration of the infringement, its intentional/negligent character, any action taken data controllers to mitigate damage to data subjects, the degree of responsibility of the controller/processor, any relevant previous infringements, and how the supervisory authority became aware of the infringement (e.g. were they notified, and to what extent, by the data controller). The risk-based approach to the imposition of this stark sanction encourages data controllers to be more responsible given that risk-averse conduct will be considered a mitigating factor when determining if, and to what extent, a fine should be imposed. Furthermore, the deterrent effect of these high fines may result in creating a level playing field, thereby enabling data controllers (e.g. IoT stakeholders) to establish a culture of privacy-by-design and default "without being pushed out of the market".[196]

**4. Conclusion**

It cannot be overstated that the GDPR only goes so far in providing for a culture of compliance within the IoT ecosystem where the value of privacy and security is meaningfully recognised and thereby adequately protected. This new EU data protection law is an evolving framework, not a silver bullet. Hence, the GDPR has the potential to be a port in the data-sharing storm for individuals, IoT stakeholders, policymakers, data protection authorities, and civil society, in providing some clear regulatory obligations that should (if adequately implemented and enforced) will enhance the certification and security of IoT devices and systems.

This impact will depend on three main factors. First, much of the GDPR's influence will turn on the manner and extent to which IoT stakeholders approach their implementation of the GDPR's key provisions in practice. In other words, will this accountability-based regime be complied with to an adequate standard or approached as merely a tick-box exercise in terms of minimum levels of compliance by those responsible in the data-sharing storm of the IoT? Given the entry into force of the GDPR this year, it remains to be seen for now if IoT stakeholders will comply to an adequate and meaningful standard to the principles, safeguards, and procedural obligations of the GDPR. Much responsibility then depends particularly on the capacity of data controllers to monitor and ensure compliance by all of the other IoT stakeholders with their obligations in the data supply chain given the significant vulnerability of the overall connected system. Secondly, data protection authorities also have a major role to play in the adequate enforcement and monitoring of the different responsibilities that should be allocated to those IoT stakeholders who make significant decision-making with regard to the processing of personal data. In other words, regulators need to pay careful attention in identifying whether processors are in fact making decisions of such importance that they should actually be reclassified as having the role (and crucially the responsibilities and liabilities) of a 'joint controller'.

Furthermore, what will be essential to IoT stakeholders in adequately undertaking these obligations, and meeting other key requirements under the GDPR, will be the clarity (and consistency) of guidance and opinions provided by the European Data Protection Board (EDPB) and national data protection authorities generally. This will be particularly important with respect to the certification of standards for IoT devices and systems. The EDPB will need to ensure that its approach to certification approval is up to date with the most recent technological advances in the IoT and that these

[196] Hildebrant (n 75), 17.

standards have been informed by evidence-based research on the actual use and operation of the IoT in practice. This will be especially important with respect to monitoring the conduct of IoT stakeholders who are often slow to adopt new standards and rely on outdated hardware and software (otherwise referred to as 'legacy systems').[197] The speed of such technical developments will make this task challenging and invariably highlights the need for an ongoing and evidence-based multi-stakeholder dialogue between DPAs, government, industry, and academia when undertaking the testing or updating of such standards. The benefits, however, could allow for the development of IoT systems that identify awareness around the areas of risk for data privacy and security. This research would thereby enable better implementation of the GDPR principles of Data Protection by Design and Default that maximise privacy and minimise data leakage by default and the development of interfaces that empower users to be able to better understand, monitor, and control the flow of personal data in their homes.[198]

[197] Y. Amar et al, "An Analysis of Home IoT Network Traffic and Behaviour", March 2018, arXiv:1803.05368v1: <https://arxiv.org/abs/1803.05368> accessed 2 July 2018.
[198] L. Urquhart et al (n 28); Y. Amar et al, "An Analysis of Home IoT Network Traffic and Behaviour", March 2018, arXiv:1803.05368v1: <https://arxiv.org/abs/1803.05368> accessed 2 July 2018.