How the EU’s General Data Protection Regulation Will Protect Consumers Using Smart Devices

Michael L. Rustad*

I. INTRODUCTION

There is confusion over which data protection rules should apply to emergent technologies, such as artificial intelligence, 3D printing, virtual and augmented reality, robots, and smart devices. The privacy concerns that these emergent technologies raise are qualitatively different than those raised by earlier technologies, such as the telephone. For instance, companies are capable of collecting data about a consumer’s everyday life on an unprecedented level because the connected devices in a smart home are interconnected in a single network. Thus, the entire system’s cybersecurity may be compromised if a single product’s weak security is breached.

Smartphones, personal fitness trackers, smart televisions, and smart appliances produce substantial amounts of sensitive information, including browsing habits, purchasing patterns, real-time location, and personal health information.1 Smart devices are autonomous, continuously harvesting, storing, and processing data without user control.2 The Internet of Things (IoT) is rapidly evolving into the Internet of Everything, connecting consumer products ranging from alarm clocks to smart meters to driverless cars.3 The ability of these devices

*  Michael L. Rustad, Ph.D., J.D., L.L.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property (IP) Law Concentration at Suffolk University Law School. He is the author of sixteen books and more than sixty law review articles. His most recent books are: GLOBAL INFORMATION TECHNOLOGIES: ETHICS AND THE LAW (2018), GLOBAL INTERNET LAW (2d ed. 2016), SOFTWARE LICENSING: PRINCIPLES AND PRACTICAL STRATEGIES (3d ed. 2016), and GLOBAL INTERNET LAW IN A NUTSHELL (3rd ed. 2015). He was appointed as editor of Computer Contracts: Negotiating and Drafting, which is a five-volume treatise on computer law published by Matthew Bender. I would like to acknowledge the research and editorial assistance of Elizabeth Saylor and Oliver Stark. I would also like to thank Matthew Rosencranz, my Suffolk University Law Review editor, and Eric Tollar, Lead Articles Editor, who organized the Internet of Things Symposium for which this piece was written. Thanks also to my faculty assistant Seth Markley for his formatting and editing assistance in preparing this article.


2. See id. (explaining how technology collects private information from everyday products).

to continuously collect and process data has raised a variety of privacy and security dilemmas because IoT devices are marketed and sold globally.4

IoT makers create “devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet.”5 These smart device makers determine how much data devices collect, the interface with users, and whether data is shared with third parties.6 The European Union’s (EU) General Data Protection Regulation (GDPR),7 which went into effect on May 25, 2018, will affect many IoT makers offering their products to EU consumers, regardless of whether these IoT makers are not located in Europe directly, because this new data protection law has an expansive extraterritorial effect.8 The GDPR not only applies to organizations that process data in the EU, but also to any number of organizations outside of the EU either offering goods or services to EU consumers or monitoring the behavior of any data subject located in any of the twenty-eight signatories to the EU treaties (Member States).9 The GDPR updated EU Data Protection law displacing the Data Protection Directive of 1995 (DPD).10

[C]onnect to the Internet—being Internet Protocol (IP) based—but may also be deployed in stand-alone IP networks not connected to the Internet. . . . With their sensor and activation capabilities, they establish relationships between the digital and physical worlds that did not previously exist. IoT includes the functions that allow users and organizations to analyze and understand the data gathered and actions taken by the things.

Id.


How much data will I need to collect? Will collecting this data add a lot of value? What should I allow users to control? What is the expected interaction? What additional features can I add to the device that will exponentially increase what can be done with the product? What benefit will be derived by opening up my device to third parties to control? What coordination can other devices have with mine to create unique experiences?

Id.


8. Id. art. 3.

9. Id.

10. See Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 (EC) [hereinafter DPD]; see also GDPR, supra note 7, art. 94.
Part II of this Article defines “IoT” and identifies both unique privacy and security risks created by continuously connected IoT devices. Part II further identifies the key privacy and security issues that the IoT poses, with a close examination of the DPD’s Article 29 Working Party. Part II concludes that the IoT industry has yet to agree upon privacy and security standards for devices, and weak or nonexistent security standards endanger consumer privacy. Part III then explores the likely impact of the GDPR on IoT’s Privacy by Design. The GDPR’s net effect will ratchet up data protection for smart devices worldwide. All IoT makers targeting EU end-users must design privacy into their devices to protect the rights of the data subject. IoT devices are cross-border by definition, and therefore, all smart device makers must be GDPR compliant.

Because the GDPR will extend to IoT devices and their networks, controllers and processors will need to achieve compliance. It is unclear how IoT makers will invest data subjects with GDPR rights—such as documenting consent—because some IoT devices do not have graphical interfaces. A study of how EU privacy and data protection law will impact IoT makers—especially those targeting consumers in the EU—is required as the EU is the largest trade partner for eighty countries.

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union.

Although growth is projected to be slow, the EU remains the largest economy in the world with a GDP per head of €25,000 for its 500 million consumers. The EU is the world’s largest trading block. The EU is the world’s largest trader of manufactured goods and services. . . . The EU is the top trading partner for [eighty] countries.
II. PRIVACY AND SECURITY RISKS UNIQUE TO THE IOT

A. What is the IoT?

The IoT “refers to the billions of physical devices around the world that are now connected to the internet, collecting and sharing data.”\(^\text{21}\) The digital intelligence of these devices enables them to communicate without human intervention, and combine the digital and physical realms.\(^\text{22}\) The IoT, the latest frontier, includes physical objects embedded with sensors or actuators that are connected to a network.\(^\text{23}\) Smartphones and devices that can connect to the IoT have the ability to control and interact with other devices connected to the IoT. “Some IoT companies even claim that their devices can ‘learn’ user behavior and adapt to them.”\(^\text{24}\)

The IoT is “integrated into the world-wide network that covers almost everything and could be available anywhere.”\(^\text{25}\) Scholars predicted that by the end of 2018, “it [would] be nearly possible to connect virtually every device on earth. Of course, most devices won’t be connected with each other due to cost constraints.”\(^\text{26}\) Nevertheless, internet-enabled cameras, baby monitors, thermostats, health-monitoring bracelets, smart refrigerators, and (eventually) driverless cars are increasingly used to record, send, and receive data.\(^\text{27}\) By 2020,

---


\(^{22}\) See id.

\(^{23}\) See BRUCE SCHNEIER, CLICK HERE TO KILL EVERYBODY: SECURITY AND SURVIVAL IN A HYPERCONNECTED WORLD 5 (2018). “The name given to this ubiquitous connectivity is the [IoT] . . . . define[d] . . . as ‘the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.’” Id. (quoting Internet of Things, GARTNER IT GLOSSARY, https://www.gartner.com/it-glossary/internet-of-things/ [https://perma.cc/77WQ-JX3R]).


Most home automation devices are constantly connected and may transmit data back to the manufacturer.

Obviously, domotics raise specific data protection and privacy challenges as an analysis of usage patterns in such a context is likely to reveal the inhabitants’ lifestyle details, habits or choices or simply their presence at home.
the number of IoT devices on the market is expected to reach more than 30 billion. Soon, virtually every electronic device will be part of a global infrastructure:

[I]n 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. As the IoT relies on the principle of the extensive processing of data through these sensors that are designed to communicate unobtrusively and exchange data in a seamless way, it is closely linked to the notions of "pervasive" and "ubiquitous" computing.29

"IoT devices connect through computer networks to exchange data with the operator, businesses, manufacturers, and other connected devices, mainly without human interaction."30 IoT controls "everything from factory equipment to traffic lights and household appliances through the Web, creates vast opportunities for improved efficiency and convenience."31

The paradox of the open Internet is that it systematically crosses national borders and disregards traditional consumer privacy everywhere. "Surveillance cameras, data brokers, sensor networks, and 'super cookies' record how fast we drive, what pills we take, what books we read, what websites we visit."32 The development of the IoT means makers have a duty to collect and process personally identifiable data, "adopting privacy and data security best practices, only collecting consumer information with express consumer consent, and providing consumers with access to their data."33


1. The EU

The EU consists of twenty-eight Member States that pool their sovereignty to work together in a unified approach, allowing the EU to take the lead in harmonizing data protection law for the information age.34 “The decision to pool the coal and steel industries of” Belgium, Germany, France, Italy, Luxembourg, and the Netherlands “brought into force by the Treaty of Paris in 1951, marked the first step towards European integration. The treaties of Rome of 1957 strengthened the foundations of this integration and the notion of a common future for the six European countries involved.”35 The Common Market was called the European Economic Community between 1957 and 1993.36 “The term also refers to the ‘European Communities,’ which originally comprised the European Economic Community (EEC), the European Coal and Steel Community (ECSC; dissolved in 2002), and the European Atomic Energy Community (Euratom).”37 “A further [twenty-two] countries have since joined the EU, including a historic expansion in 2004 marking the re-unification of Europe after decades of division.”38

2. Overview of the DPD

The DPD gives data subjects control over the collection, transmission, or use of personal information.39 “Directives require EU countries to achieve a certain result, but leave them free to choose how . . . EU countries must adopt measures to incorporate [directives] into national law . . . to achieve the [directive’s] objectives.”40 The DPD requires each of the twenty-eight Member States to enact national legislation that protects “the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of
personal data." Member States are free to enact national legislation that offers data subjects more privacy protection than the minimum dictates of the DPD.

The DPD defines the processing of personal data to mean all automatic or non-automatic operations on personal data including the “collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction” of data. The DPD confers controllers with determining the “purposes and means of the processing of personal data” determined by community laws or regulations. In contrast, processors do the actual processing of data under the direction of controllers.

The scope of the DPD encompasses the processing of personal data wholly or partly by automatic means where the data forms a file. Some processing is outside the DPD’s sphere of application, including public security, defense, state security, and criminal law investigations. Many of the DPD provisions establishing data subject rights and limitations on the processing of data were adopted by the GDPR. The DPD adopted a data minimization principle that data be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.” The principal difference between the GDPR and the DPD is that the DPD required each EU Member State to develop national legislation to address the processing of personal data.

In contrast, the GDPR was a single regulation applying automatically to all EU Member States. The DPD applies where a controller carries out activities in any Member State territory. If an IoT controller is located in several Member States, it must comply with the national data protection regulations of each.

41. See DPD, supra note 10, art. 1(1).
42. See id. art. 4.
43. See id. art. 2(b).
44. See id. art. 2(d).
45. See DPD, supra note 10, art. 2(e).
46. See id. art. 3(1).
47. See id. art. 3(2).

The GDPR supersedes the [DPD] and will fully phase out the DPD and become national law for all EU Member States by May 25, 2018. The GDPR builds on the key tenets of the DPD with more specific data protection requirements, a global scope, and stiffer enforcement as well as non-compliance penalties. As a result, citizens will have more control over their personal data and more recourse if personal data is misused, while data controllers and processors will be required to protect sensitive personal data by design. Finally, the GDPR offers a much simpler regulatory environment for businesses that collect or process EU citizens’ and residents’ personal data.

49. See DPD, supra note 10, art. 6(b).
50. See id. art. 4.
51. See id. art. 4(b).
country to comply with the DPD. Article 29 of the DPD created the WP29, which “provide[s] the European Commission with independent advice on data protection matters and help[s] in the development of a harmonized implementation of data protection rules in the EU Member States.” The WP29 is composed of representatives of the national supervisory authorities in the Member States, a representative of the European Data Protection Supervisor (EDPS), and a representative of the European Commission to provide the secretariat.

3. The WP29 Study of IoT Privacy and Security Risks

The DPD created the WP29 to determine policies for processing data and to advise the European Commission on privacy policies. The WP29 served as “an independent European advisory body on data protection and privacy.” The WP29 must determine “the level of protection in the Community and in third countries” and report to the Commission. The WP29 reports any “divergences likely to affect the equivalence of protection for persons with regard to the processing of personal data in the Community are arising between the laws or practices of Member States.” The WP29 creates an “annual report on the situation regarding the protection of natural persons with regard to the processing of personal data in the Community and in third countries,” which it shares with the Commission, the European Parliament, the Council, and the general public. Prior to the GDPR, IoT stakeholders were required to comply with the DPD rules for protecting data subjects. These DPD rights extended to subscribers of IoT services, device owners, and “any individual whose personal data [was] processed.”

52. See id. recital 19.
56. See WP29, Opinion 8/2014, supra note 27, at 1 (“[WP29’s] tasks are described in Article 30 of [the DPD] and Article 15 of Directive 2002/58/EC.”).
57. See DPD, supra note 10, art. 30(1)(b).
58. See id. art. 30(2).
59. See id. art. 30(6).
60. See WP29, Opinion 8/2014, supra note 27, at 19.
61. See id.
Even though the GDPR supplanted the WP29 on May 25, 2018, the Opinion 8/2014 on the Recent Developments on the IoT published by the WP29 (WP29 Opinion) is the most comprehensive policy analysis of the risks of the IoT on data protection and privacy. The WP29 Opinion was to ensure that the industry “respect the many privacy and security challenges which can be associated with the IoT.” IoT controllers rarely give end-users “access to the raw data” harvested by devices. The key attribute of the IoT is Internet connectivity to automatically send and/or receive data. The WP29 Opinion targets wearable devices containing sensors to extend functionality, quantified self or smart devices worn by persons to record information about their habits and lifestyles, and home automation such as connected refrigerators and thermostats. The WP29 identified significant privacy and data protection challenges amplified by the “exponential increase of data processing involved by its evolution.” The IoT connects tens of millions of devices affecting:

[E]very aspect of our lives because they are things like cars, home appliances, thermostats, light bulbs, fitness trackers, medical devices, smart streetlights and sidewalk squares. Many of these devices are low-cost, designed and built offshore, then rebranded and resold. . . .

. . . The owners of those devices don’t care. They wanted a webcam—or thermostat, or refrigerator—with nice features at a good price. Even after they were recruited into this botnet, they still work fine . . . . The sellers of those devices don’t care: They’ve already moved on to selling newer and better models.

Wearable devices include “embed cameras, microphones and sensors that can record and transfer data to the device manufacturer.” “Some of the self-tracker systems (e.g. pedometers, sleep trackers) on the market also suffer from security flaws allowing attackers to tamper observed values that are reported to the

---

63. See WP29, Opinion 8/2014, supra note 27, at 3.
64. See id. at 19.
67. Id. at 6.
69. See WP29, Opinion 8/2014, supra note 27, at 5.
It is crucial that these devices offer data protection, especially if they are used for health-related reasons.\(^{71}\)

The application programming interfaces for these wearable devices, such as Android Wear, “also support[] the creation of applications by third parties who can thus get access to the data collected by those things.”\(^{72}\) Other examples include wearable health devices that monitor weight, pulse, and other health measures.\(^{73}\) These devices can, for example, quantify the “effects of the physical activity based on predefined thresholds and the likely presence of disease symptoms, to a certain extent.”\(^{74}\) Quantified self sensors are employed for specific situations. “For example, an accelerometer placed at the belt of a data subject, with the appropriate algorithms, could measure the abdomen moves (raw data), extract information about the breathing rhythm (aggregated data and extracted information) and display the level of stress of the data subject (displayable data).”\(^{75}\)

The WP29 Opinion contends that data controllers “should offer an option to disable the ‘connected’ feature of the thing and allow it to work as the original, unconnected item (i.e. disable the smart watch or glasses connected functionality).”\(^{76}\) It is unclear how IoT makers would be able to give data subjects a mechanism for disabling connectivity for smart devices already in the field.\(^{77}\) IoT makers have created mechanisms for updated terms of use for smart devices.\(^{78}\) However, a “Chinese smart device manufacturer, Yeelight, sent a message to users that its light bulbs no longer functioned properly as a result of GDPR compliance.”\(^{79}\)

Home-automation devices include “‘connected’ light bulbs, thermostats, smoke alarms, weather stations, washing machines, or ovens that can be controlled remotely over the [I]nternet.”\(^{80}\) These home-automation devices continuously harvest data and transmit that data back to the manufacturer.\(^{81}\) The WP29 Opinion notes that home-automated devices “raise specific data protection

---

70. See id. at 19.
71. See id.
72. Id. at 5.
73. See WP29, Opinion 8/2014, supra note 27, at 5.
74. See id.
75. Id.
76. See id. at 20. “The Working Party has already specified that data subjects should have the possibility to ‘continuously withdraw (their) consent, without having to exit the’ service provided.” Id.
77. See WP29, Opinion 8/2014, supra note 27, at 21 (noting developments allowing measured control of consent in progress).
79. Id.
81. See id.
and privacy challenges as an analysis of usage patterns in such a context is likely to reveal the inhabitants’ lifestyle details, habits or choices or simply their presence at home.”

4. Chief IoT Privacy Risks

a. IoT Users’ Lack of Control

The lack of control IoT users have over their personal information is a challenging dilemma attributable to information asymmetry. The IoT provider has all of the information about data collection whereas the user does not know what information the provider harvests. IoT devices often do not have graphical user interfaces that enable user interaction. Third party monitoring of pervasive services is ubiquitous and not perceptive by users.

An IoT user “lose[s] all control on the dissemination of his/her data, depending on whether or not the collection and processing of this data will be made in a transparent manner or not.” “Third parties other than device manufacturers and third party application developers may use IoT devices to collect and process information about individuals.” For instance, health-insurers may wish to give pedometers to customers to monitor how often they exercise and adapt their insurance premiums accordingly.

Traditional mechanisms of notice and consent do not mesh well with IoT data flows between objects and back-end systems. At present, IoT device users have no opportunity to review and consent to what data connected devices collect and

82. Id.
83. See id.
84. See WP29, Opinion 8/2014, supra note 27, at 6. “Asymmetric information, also known as information failure, occurs when one party to an economic transaction possesses greater material knowledge than the other party.” Julia Kagan, Asymmetric Information, INVESTOPEDIA, https://www.investopedia.com/terms/a/asymmetricinformation.asp [https://perma.cc/VD2P-C3WF].
86. See WP29, Opinion 8/2014, supra note 27, at 6. The New York Times reported that applications are tracking users’ daily habits and the information is sold to dozens of companies, reporting that “[t]hese companies sell, use, or analyze the data to cater to advertisers, retail outlets and even hedge funds seeking insights into consumer behavior.” Jennifer Valentino-DeVries et al., Your Apps Know Where You Were Last Night, And They’re Not Keeping it Secret, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/3TAH-RXXZ].
88. See id. at 12.
89. See id. at 6.
In the IoT environment, “communication between objects can be triggered automatically as well as by default, without the individual being aware of it.”\textsuperscript{91} The WP29 Opinion states:

In the absence of the possibility to effectively control how objects interact or to be able to define virtual boundaries by defining active or non-active zones for specific things, it will become extraordinarily difficult to control the generated flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.\textsuperscript{92}

\subsection*{b. Quality of Users’ Consent}

IoT makers have not developed a way to get user consent, which is the main “legal basis that should be principally relied on in the context of the IoT, whether by device manufacturers, social or data platforms, devices lenders or third party developers.”\textsuperscript{93} Many IoT users will be unaware that specific objects are carrying out data processing.\textsuperscript{94} The IoT industry’s failure to obtain valid consent violates EU data protection law on informed consent.\textsuperscript{95} The DPD allowed Member States to process personal data “only if: [T]he data subject ha[d] unambiguously given his consent” or a well-defined exception existed.\textsuperscript{96}

Neither the DPD nor the GDPR provides guidance on how IoT providers are to obtain valid consent. The WP29 Opinion observes that smart watches differ from nonconnected ones in not providing signals to the user they are connected to.\textsuperscript{97} Smart device embed “cameras, microphones, and motion sensors that can record and transfer data without” the user consenting to such processing.\textsuperscript{98} This casts doubt on data processing identification through “Wearable Computing, which might be solved by envisaging appropriate signposting that would be actually visible to the data subjects.”\textsuperscript{99}

IoT makers should design signposts on their devices that would make data subjects aware of data processing.\textsuperscript{100} Data subjects should have the means to reject certain data processing to comply with EU consent requirements.\textsuperscript{101}

\begin{flushright}
\textsuperscript{90} See id.
\end{flushright}
\begin{flushright}
\textsuperscript{91} WP29, Opinion 8/2014, supra note 27, at 6.
\end{flushright}
\begin{flushright}
\textsuperscript{92} Id.
\end{flushright}
\begin{flushright}
\textsuperscript{93} Id. at 15.
\end{flushright}
\begin{flushright}
\textsuperscript{94} See id. at 7.
\end{flushright}
\begin{flushright}
\textsuperscript{95} WP29, Opinion 8/2014, supra note 27, at 7.
\end{flushright}
\begin{flushright}
\textsuperscript{96} See DPD, supra note 10, art. 7(a)-(f) (requiring consent or statutory exceptions where personal data potentially processed without data subject’s consent).
\end{flushright}
\begin{flushright}
\textsuperscript{97} See WP29, Opinion 8/2014, supra note 27, at 7.
\end{flushright}
\begin{flushright}
\textsuperscript{98} See id.
\end{flushright}
\begin{flushright}
\textsuperscript{99} Id.
\end{flushright}
\begin{flushright}
\textsuperscript{100} See id.
\end{flushright}
\begin{flushright}
\textsuperscript{101} WP29, Opinion 8/2014, supra note 27, at 7.
devices are not designed to provide disclosures about what data is collected or the mechanisms for obtaining consent.  

c. Inferences Derived from Repurposing Data

“The interaction between the device and the data is far from simple, involves numerous parties and, under the GDPR, responsibility for the data extends across the whole supply chain.” The WP29 Opinion noted how seemingly innocuous data gathered for one purpose could “be used to infer other information with a totally different meaning (e.g. the individual’s driving habits).” IoT users may consent to the sharing of personal data for one purpose but not be willing to “share this secondary information that could be used for totally different purposes.” The WP29 Opinion contends that “it is important that, at each level (whether raw, extracted or displayed data), IoT stakeholders make sure that the data is used for purposes that are all compatible with the original purpose of the processing and that these purposes are known to the user.”

Wearable IoT devices with multiple sensors can be worn on the body to predict when the elderly are about to fall. “Wearables and other sensors can act as a caretaker’s eyes and ears to observe what is going on in an older individual’s home at any time, but it’s what is done with this information that can make the data particularly valuable.” The benefits of health wearables are undeniable, but there needs to be safeguards against misuses by third parties. “Examples of misuse vary from users’ data sale without informing them to data breaches due to lack of protection measures.” “Companies and shopping malls can purchase personal data of IoT . . . analyzing the personal preferences of consumers, shooting the arrow at the target to accomplish accurate marketing.” European data protection law requires data subject consent prior to data being transferred to third parties.

102. See id.
103. See Brar, supra note 18.
105. Id. at 8.
106. Id.
110. See Nekrutenko, supra note 108.
d. Intrusive Behavior Patterns and Profiling

Sensors and Radio Frequency Identification Devices (RFID) “will enable the objects to interact but[,] due to the huge ratio of objects and their variations[,] creates the scalability and diversity of objects.”\textsuperscript{111} IoT makers will need to determine how the provisions of the GDPR govern their RFID devices that are used given these tracking technologies because RFID can be deployed as a device to track customers’ movement. Some argue that RFID is exempted from GDPR compliance.\textsuperscript{112}

The WP29 Opinion states how different IoT objects incorporating sensors can be combined to detect data subject patterns of habits and behaviors, thus enabling profiling.\textsuperscript{113} Connected devices “might enable the detection of an individual’s even more detailed and complete life and behavio[r] patterns.”\textsuperscript{114} The concern is that surveillance might reach the “private sphere of the individuals’ life, including homes.”\textsuperscript{115} If people are under constant surveillance, then it would cause changes in their individual behaviors.\textsuperscript{116}

e. IoT Undermines Secrecy in the Back Stage

Sociologist Erving Goffman’s dramaturgical theory of the presentation of self draws upon Shakespeare’s \textit{All the World’s a Stage}.\textsuperscript{117} The dramaturgical perspective highlights how we use impression management “in the establishment, and the identity and interrelationships of the several performance teams which operate in the establishment.”\textsuperscript{118} Goffman explains the division between the back region, where the performance of a routine is prepared, and the front region, where the performance is presented.\textsuperscript{119} It is the front stage where “accentuated facts make their appearance” from the “backstage—where the suppressed facts make an appearance.”\textsuperscript{120} Impression management can be seen “the moment when a performer leaves the back region and enters the place where the audience is to be found.”\textsuperscript{121}

Goffman illustrates the manifold ways that front and back regions are divided with his description of the backstage of the bedroom, kitchen, and bathroom.\textsuperscript{122}

\begin{footnotes}
\item 111. See Haroon et al., supra note 25, at 253.
\item 112. See id.
\item 113. See WP29, Opinion 8/2014, supra note 27, at 8.
\item 114. Id.
\item 115. Id.
\item 116. See id.
\item 117. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 135 (1956).
\item 118. Id. at 154.
\item 119. See id. at 152.
\item 120. Id. at 69.
\item 121. GOFFMAN, supra note 117, at 74.
\item 122. See id. at 75.
\end{footnotes}
He notes how a glance into a restaurant, store, or home, a few minutes before these establishments are opened reveals the front and back regions. The backstage may be defined as a place, relative to a given performance, where the impression fostered by the performance is knowingly contradicted as a matter of course. The backstage gives “the performer some privacy in which to prepare himself for the show.” It is in the backstage where we “can relax; [we] can drop [our] front, forgo speaking [our] lines and step out of character.” “Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development,” and “is one of the resources that situated subjects require to flourish.” At its most basic level, the right to privacy is the right to control access to the backstage. Privacy is the right of an individual to decide how and when backstage information can be revealed to what parties under what conditions.

The widespread use of IoT devices blurs the distinction between front and back regions crucial to controlling the borderline between the metaphorical frontstage and backstage. The IoT represents “a shift from ‘active’ to ‘passive’ data production,” transforming the individual to effectively become “a core part of the machine itself, a machine that is designed to be parasitic on human action.” Wearable things influence “the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.” Wearable devices make it difficult to control access to front stage and back stage regions as identifiers are being harvested at all times.

Fitness trackers undermine military secrets “about the location and staffing of military bases and spy outposts around the world ha[ve] been revealed by a fitness tracking company.” Strava—a fitness tracking company—released a map with more than three trillion individual GPS data points where their fitness application was used, “including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote As suggested, the bathroom and bedroom, in all but lower-class homes, are places from which the downstairs audience can be excluded. Bodies that are cleansed, clothed, and made up in these rooms can be presented to friends in others. In the kitchen, of course, there is done to food what in the bathroom and bedroom is done to the human body.

Id.

123. Id. at 77.
124. Id. at 69.
125. GOFFMAN, supra note 117, at 157.
126. Id. at 70.
129. See WP29, Opinion 8/2014, supra note 27, at 8.
areas who have unusual exercise patterns.”

IoT devices trace “digital footprints that echo the real-life steps of individuals,” thus “each person’s connection to online services and personal devices makes it increasingly difficult to keep secrets.” As such, we too often think that “secrets lie hidden, when now they are mostly out in the open.”

Protecting the back stage becomes challenging because IoT devices “are connected to different types of devices and this increase in connectivity and data collection results in less control.” The WP29 Opinion notes how the interconnections between multiple sensor devices creates unique digital “fingerprints and more stable identifiers which IoT stakeholders will be able to attribute to specific individuals.” The misuse of digital fingerprints and other information through including location and movement analytics is enabled data by information technologies that can combine this information “with other data issued from other systems (e.g. CCTV or Internet logs).”

f. IoT Security Issues

IoT makers have not paid much attention to privacy and security, but now must incorporate privacy “by design and by default.” At present, devices comprising the IoT are particularly vulnerable to data theft due to the lack of industry security standards. The European Commission will not allow EU consumer data to be exported between Europe and the United States unless it is protected by reasonable security standards that are not “absent or immature[].”

The regulatory environment for IoT—like the security environment—is immature and shot through with contradictions. Technology focused businesses, like nature, abhor a vacuum. But they abhor regulations even more, even when the establishment of some standards might clarify the risk factors and lead to an accelerating expansion of use cases and market adoption. Such is the case today with GDPR and IoT.

131. Id.
132. See id.
134. Id. (quoting Peter Singer, strategist and senior fellow at Washington D.C. think tank).
135. See Internet of Things (IoT), supra note 33.
137. Id.
138. See GDPR, supra note 7, art. 25 (entitling GDPR data protection by design and by default).
nonexistent or inadequate.\textsuperscript{140} IoT-connected objects are particularly vulnerable to data theft due to the lack of industry security standards.\textsuperscript{141}

The most common IoT vulnerabilities are privilege escalation, eavesdropping, brute-force password attacks, malicious node injection, firmware hijacking, denial of service attacks, and physical tampering.\textsuperscript{142} An example of the vulnerabilities in these IoT-connected devices can be found in defective software in relatively autonomous automobiles have known exploitable vulnerabilities. \textit{Wired} reported a lawsuit arising out of a remote hack of a Chrysler Jeep, in which software developers took control of a moving vehicle through its Internet-connected “infotainment” system.\textsuperscript{143} If an IoT maker fails to update its products to counter new malware, is the IoT maker liable for customer losses due to a cyber intrusion?

The WP29 Opinion notes that it is unclear how IoT makers will “balance battery efficiency and device security.”\textsuperscript{144} IoT makers risk turning everyday objects “into a potential privacy and information security target while distributing those targets far more widely than the current version of the Internet.”\textsuperscript{145}

5. Overview of the EU’s GDPR

On May 25, 2018, the European Commission published the GDPR, which replaced the DPD.\textsuperscript{146} The GDPR automatically applies to all of the European Economic Area (EEA) Members and requires no national legislation.\textsuperscript{147} The

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{141} The IoT lacks well-established overarching standards that describe how the different parts of the technology stack should interact. Instead, large players and industry organizations use their own solutions. Some segments, such as industrials, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years.
\item \textsuperscript{142} Manuel Nedbal, \textit{IoT Insecurity: 6 Common Attacks and How to Protect Customers}, Channel Partners, https://www.channelpartnersonline.com/blog/iot-insecurity-6-common-attacks-and-how-to-protect-customers/ [https://perma.cc/3MW8-PZAF].
\item \textsuperscript{144} See WP29, Opinion 8/2014, supra note 27, at 9.
\item \textsuperscript{145} Id.
\item \textsuperscript{146} See GDPR, supra note 7.
\end{itemize}
\end{footnotesize}
EEA includes the twenty-eight EU countries “and also Iceland, Liechtenstein and Norway. It allows them to be part of the EU’s single market.”\textsuperscript{148} The EU Commission proposed the GDPR as a regulation—a legal instrument binding in all of its parts; more importantly, the GDPR is self-executing, which means that it is immediately enforceable as law in all Member States.\textsuperscript{149}

III. GDPR PROVISIONS IMPACTING THE IOT INDUSTRY

A. The GDPR’s Sphere of Application

IoT is an interconnected digital network that employs: “unique identifiers in the form of an IP address which . . . have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment.”\textsuperscript{150} The GDPR lays out EU data protection rules for the processing of personal data that apply to IoT devices.\textsuperscript{151} “Smartphones that interact with other smartphones, vehicle-to-vehicle communication, connected video cameras, and connected medical devices” all illustrate connected products.\textsuperscript{152}

IoT products qualify as automated means in that they harvest and process users’ personal information.\textsuperscript{153} Smart devices “communicate with consumers, collect and transmit data to companies, and compile large amounts of data for third parties.”\textsuperscript{154} Personal data from IoT devices may be statistically analyzed to develop analytics based upon correlations tailoring links specific to the data subject’s interests, behaviors, habits, and personality.\textsuperscript{155} Unlike humans, IoT devices “do not ask permission to ingest, feed, or store it, nor provide any way for the database to reverse engineer the process and conduct spot audits.”\textsuperscript{156}

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{148} Countries in the EU and EEA, GOV.UK, https://www.gov.uk/eu-eea [https://perma.cc/84G8-5L6K].
  \item \textsuperscript{149} See Types of EU Law, EUR. COMMISSION, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en [https://perma.cc/GX75-Q77F]. “Regulations are legal acts that apply automatically and uniformly to all EU countries as soon as they enter into force, without needing to be transposed into national law. They are binding in their entirety on all EU countries.” Id.
  \item \textsuperscript{151} See GDPR, supra note 7, art. 1(1).
  \item \textsuperscript{152} See Internet of Things (IoT), supra note 33.
  \item \textsuperscript{153} Crabtree & Mortimer, supra note 128, at 1. “The Internet of Thing (IoT) further complicates the situation, reshaping the nature of data collection from an ‘active’ feature of human-computer interaction to a ‘passive’ one in which devices seamlessly communicate personal data to one another across computer networks.” Id.
  \item \textsuperscript{154} See Internet of Things (IoT), supra note 33.
  \item \textsuperscript{156} See MORAN & PANAGOS, supra note 138, at 4.
\end{itemize}
\end{footnotesize}
2. The GDPR’s Long-Arm Jurisdictional Reach

The territorial scope of the GDPR is defined as the “processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.”\textsuperscript{157} The GDPR has an expansive extraterritorial impact applying to all companies headquartered in the United States (and all other non-EU countries) processing both the personal and sensitive data of data subjects residing in the EU.\textsuperscript{158} EU-based companies must comply with the GDPR because they process data “in the context of the activities of an establishment . . . in the Union.”\textsuperscript{159} Companies located any other place in the world must comply with the GDPR because they offer goods or services to persons in the EU or monitor the behavior of persons located in the EU.\textsuperscript{160} Unlike the DPD, the GDPR has no requirement that an entity be located in the EU.\textsuperscript{161} Companies located anywhere in the world are subject to the GDPR if they provide goods or services to or monitor persons residing in Europe.\textsuperscript{162}

The GDPR only provides protections for natural persons as opposed to legal persons such as corporations.\textsuperscript{163} All companies or entities with an establishment in the EU must comply with the GDPR.\textsuperscript{164} Antmicro, a Swedish company, “is an embedded software and product development firm.”\textsuperscript{165} ProSyst, a Bosch acquisition, is a German IoT provider that offers IoT gateway software solutions.\textsuperscript{166} IoT Analytics, a German company, is also an IoT market research company subject to the GDPR.\textsuperscript{167} Most of the world’s leading IoT makers are headquartered outside the EU.\textsuperscript{168} However, some non-EU companies, such as LinkedIn, PayPal, Amazon, Twitter, and Zynga, established branches in the

\begin{footnotesize}
\begin{itemize}
  \item \textsuperscript{157} GDPR, supra note 7, art. 3.
  \item \textsuperscript{158} Id.
  \item \textsuperscript{159} Id. art. 3(1).
  \item \textsuperscript{160} Id. art. 3(1)(b).
  \item \textsuperscript{161} GDPR, supra note 7, art. 3(1) (applying GDPR to processing of personal data regardless of processing location).
  \item \textsuperscript{162} Id.
  \item \textsuperscript{163} See id. art. 1(1). “This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.” Id. “This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.” Id. art. 1(2).
  \item \textsuperscript{164} Id. art. 3.
  \item \textsuperscript{165} Top Internet of Things Companies, POSTSCAPES (March 5, 2019), https://www.postscapes.com/companies/ [https://perma.cc/UXV2-NDRT].
  \item \textsuperscript{166} See id.
  \item \textsuperscript{167} See id.
  \item \textsuperscript{168} See id.
\end{itemize}
\end{footnotesize}
Silicon docks area of Dublin, Ireland. A recital to the GDPR notes that establishments include branches, subsidiaries, and other stable arrangements. Companies located anywhere in the world are subject to the GDPR if they offer goods or services, or monitor persons residing in the EU. Examples of U.S. companies without EU establishments are found in Boston—a world-leading city in innovation—where both RapidMiner, a predictive analytics company, as well as MC10 Inc., a pioneer in wearable electronics, are located. Armis, a California company, is the leading provider of IoT security platforms without an EU establishment. Bastille, too, does not have an EU establishment, and is an Atlanta company specializing in enterprise threat detection, which it calls the “Internet of Radios.”

The Silicon Valley in California is the center of sensors for consumer products, such as Invensene, as well as IoT analytics providers, such as Splunk. Zingbox, a California IoT security company, offers products for retail and health industries. Silicon Labs of Austin, Texas, “provides mixed-signal and RF CMOS silicon architectures, MCU wireless components, and sensors along with supporting software and cloud services.”

---


Welcome to the Silicon Docks, the Dublin neighborhood bordering the Grand Canal Docks, where tech giants like Google and Facebook have set down their international headquarters. Beyond the docks, other major players like LinkedIn, PayPal, Amazon, Twitter, and Zynga are all packed into a city that’s roughly one-fifth the size of San Francisco.

Id.

170. See GDPR, supra note 7, recital 22.

Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Id.

171. Id. art. 3(1)(b).

172. Id.


174. Id.


177. See Top Internet of Things Companies, supra note 165.
company, “offers lighting manufacturers end-to-end solutions for analytics, building intelligence and beacon management.”

Augury, headquartered in Israel, “builds a mechanical diagnostics solution using vibration and ultrasonic sensors,” while Ayyeka, a Jerusalem company, “offers an end-to-end industrial [IoT] platform.” Israel is also the home of 3dsignals, the developer of an acoustic sensor analytics solutions. Presenso, another Israeli IoT provider, “develops a cloud-based deep learning and machine learning platform for predictive maintenance application.” Israeli IoT providers, like any non-EU providers, are subject to the GDPR’s data protection regime to the extent that they offer goods or services to persons residing in the EU or monitor the behavior of anyone located in the EU. The GDPR asserts jurisdiction over any non-EU company that processes data whose behavior takes place in the EU.

3. GDPR’s Definitions Applied to IoT Devices

“[T]he biggest threat to privacy and security in consumer products is posed by those [IoT] devices [that] track personal data by seamlessly integrating into the consumers’ activities and lifestyles.” An IoT device “blend[s] into everyday objects, and [is] not readily discernible as an internet-connected device with the capacity to sense, collect, and transmit large-scale personal data.” The GDPR applies “if the content of communications includes some data related to a natural person ([e.g.], age, name, address) or if the device is connected to a natural person ([e.g.], cars, clothes, home devices, health devices), electronic communications content and traffic data will qualify as personal data.” The scope of the GDPR includes the processing of personal data for all users located in the EU. Personal data under the GDPR is any “information relating to an identified or identifiable natural person (‘data subject’).” As long as it

179. See Top Internet of Things Companies, supra note 165.
180. See id.
181. See id.
182. See GDPR, supra note 7, art. 3(2)(a)-(b). Non-EU companies “offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or the monitoring of their behavior as far as their behavior takes place within the Union” are subject to the provisions of the GDPR. Id.
183. See id. art. 3(1)-(2).
185. Id.
187. GDPR, supra note 7, art. 3(1).
188. Id. art. 4(1).
is a personal identifier, the GDPR definition includes a “name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”

Under the GDPR, controllers determine the how, when, and why of data processing, while processors perform “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means.” Data controllers “ensure their processor abides by data protection law and processors must themselves abide by rules to maintain records of their processing activities.” Controllers must take reasonable steps to ensure personal data is accurate; inaccurate data must be erased or rectified immediately.

Stored personal data must be retained “for no longer than is necessary,” but historical, statistical, or scientific data may be retained longer unless such storage is incompatible with the original purposes. “The immutability and the permanent storage of data stored in the blockchain so far do not seem to comply with the key principles of the GDPR.” Controllers must take reasonable steps to ensure personal data is accurate; inaccurate data is promptly deleted or corrected. Further, the GDPR requires data processing to be “adequate, relevant, and limited to what is necessary.” To comply with EU data minimization principles, IoT makers must address a variety of questions, such as how the data is collected, used, sent, and stored.

IoT controllers determine what data may be acquired by devices and sensors and for what purposes. “The processes described above can be grouped into four major stages, data move from sensors or devices to the cloud through suitable

---

189. Id.
190. Id. Under the GDPR, a controller is defined as:

[T]he natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

191. GDPR, supra note 7, art. 4(7).
193. GDPR, supra note 7, art. 5(1)(d).
194. Id. art. 5(1).
196. GDPR, supra note 7, art. 5(1)(d).
197. Id. art. 5(1)(c).
connectivity, then data processing and results or output." IoT controllers ensure the processors comply with data collection purposes. Smart devices include step counters, sleep trackers, “connected” home devices like thermostats, smoke alarms, connected glasses or watches, which continuously process personal data.

Personal data includes any “information relating to an identified or identifiable natural person (‘data subject’) [or] an identifiable natural person.” The definition encompasses a “name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.” IoT processors can often identify individuals from data harvested by devices. IoT data, for example, enables lifestyle inferences from data generated from lighting, heating, ventilation, and air conditioning. IoT data will account for ten percent of all the data registered globally in 2020. Connected cars, for example, “collect a wide range of operator and performance data.” A possible solution is to transform the customer experience, providing constant connect points between the auto maker and the consumer.

4. IoT Data Minimization

The GDPR’s data minimization principle is that data be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.” If data is further processed, it must be “for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes” and “not be incompatible with the initial purposes (‘purpose limitation”).” The IoT industry’s business model is based on data maximization to monetize data, which is antithetical to data minimization. For example, companies such as “Microsoft, Bosch, Samsung, Cisco, Fujitsu, and Orange are launching an open data marketplace” that

---


201. GDPR, supra note 7, art. 4(1).

202. Id.


204. Id.


207. GDPR, supra note 7, art. 5(1)(b).

208. Id.

209. See Upton, supra note 206.
commodify personal data by allowing sales through microfees. U.S. automobile manufacturers employ data maximization to profit from commodifying consumer data. IoT initiatives that enable the purchasing of personal data by third party data brokers violate the GDPR’s data minimization rules.

“IoT analytics combines insights obtained from a traditional approach of finding patterns within streaming data by using data warehouse mining and real-time telemetry of data points provided by individual IoT devices in the field.”

B. The Difficulty of Obtaining Consent for IoT Devices

IoT controllers have a duty “to demonstrate that the data subject has consented to the processing of his or her personal data” if processing is predicated upon consent. If an IoT controller makes a written request for consent, it must be in an “intelligible and easily accessible form, using clear and plain language.” IoT controllers need to inform data subjects of “the right to withdraw his or her consent at any time” prior to them giving consent. IoT makers find it challenging to obtain the user’s prior consent when personal data is shared with third-party application developers who “do not display sufficient information for the user’s consent to be considered as specific and sufficiently informed” to comply with EU data protection law.

1. Obtaining Consent from Children

For children below the age of sixteen, processing is only lawful if consent is given by a parent or a person with parental responsibility. IoT controllers will find it challenging to give parents the information needed to obtain verifiable consent. IoT makers that fail to obtain parental consent do so at their peril. The Children’s Online Privacy Protection Act (COPPA) protects the privacy of children under the age of thirteen. The COPPA prohibits any company to harvest

210. See Lazarevich, supra note 205.
211. See id. “Apart from participating in emerging open data markets, companies are expected to rethink their data usage and focus on extracting additional value from their IoT infrastructure. It means turning IoT data to the profit center.” Id.
212. GDPR, supra note 7, art. 5(1)(b).
vent-processing-work/ [https://perma.cc/Y4YY-YKZ7];
214. GDPR, supra note 7, art. 7(1).
215. Id. art. 7(2).
216. Id. art. 7(3).
218. GDPR, supra note 7, art. 8(1).
personally identifiable information without their parents’ consent. The Federal Trade Commission (FTC) entered into a settlement agreement with a smart toy maker in India and its U.S. subsidiary for “collecting personal information from children without providing direct notice and obtaining their parent’s consent, and failing to take reasonable steps to secure the data it collected. VTech will pay $650,000 as part of the settlement with the FTC.”

The FTC contended that VTech, the IoT toy maker, violated the COPPA by failing “to provide direct notice of information collection and use practices to parents” and by failing to provide a “link to its privacy policy in each area where personal information was collected from children.” The FTC also charged VTech with failing to implement adequate security safeguards “to protect transmitted and stored information and implementing an intrusion prevention or detection system to alert the company of an unauthorized intrusion of its network.” VTech was victimized by a cyber intrusion when “a hacker accessed its computer network and personal information about consumers including children who used its Kid Connect app.” The FTC charged that VTech misrepresented its privacy policy by claiming that most personal information of children was encrypted when it “did not encrypt any of this information.”

In 2012, the FTC settled a COPPA rule claim against RockYou for collecting information from children without obtaining parental consent and misrepresenting its privacy and security promises. The settlement order bars RockYou from making future deceptive claims, “requires it to implement and maintain a data security program, bars future violations of the COPPA rule, and requires it to pay a $250,000 civil penalty.” The FTC’s COPPA rule applies to “mobile apps that send or receive information online (like network-connected games, social networking apps, or apps that deliver behaviorally-targeted ads), internet-enabled gaming platforms, plug-ins, advertising networks, internet-enabled location-based services, voice-over internet protocol services, connected toys or other [IoT] devices.”

---

221. Id.
223. Id.
224. Id.
225. Id.
228. Id.
If IoT makers make written requests for a data subject’s consent, it must be presented “in a manner clearly distinguishable from the other matters.”\textsuperscript{230} To comply with the GDPR, an IoT maker needs “a record of the consent and how it was given, individuals have a right of withdrawal, and where consent is part of a bigger contract, transparency should be increased by flagging what is being consented to and by writing clearly in plain language.”\textsuperscript{231}

2. IoT Processing of Sensitive Personal Data

IoT devices and apps process “a myriad of sensitive data from sensors and devices connected to the hub” and there is a paucity of “basic tools and services for analyzing what they do with that information” that data subjects want to keep secret.\textsuperscript{232} An IoT application can acquire a variety of privacy-sensitive information through device state interfaces . . . that can be used to profile habits . . . and pose risks to physical privacy.\textsuperscript{233} Blockchain technologies have the potential of safeguarding sensitive information such as transmitted by health care providers.\textsuperscript{234} IoT controllers do not presently have protocols for documenting data-subject consent for categories of sensitive information.\textsuperscript{235} The GDPR prohibits processing personal data that reveals “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.”\textsuperscript{236}

The GDPR allows processing of this information if the subject gives explicit consent.\textsuperscript{237} Similarly, these data categories may be processed in the context of a collective agreement in employment, social security, and social protection as long as there are appropriate safeguards.\textsuperscript{238} Another exception is if the data subject is physically or legally incapable of giving consent and “processing is necessary to protect the vital interests of the data subject or of another natural person.”\textsuperscript{239}

\textsuperscript{230} GDPR, supra note 7, art. 7(2).
\textsuperscript{232} Z. Berkay Celik et al., Sensitive Information Tracking in Commodity IoT, in 27TH USENIX SECURITY SYMPOSIUM 1687, 1687 (2018).
\textsuperscript{233} Id. at 1690.
\textsuperscript{235} GDPR, supra note 7, arts. 9(1), 12-14.
\textsuperscript{236} Id. art. 9(1).
\textsuperscript{237} Id. art. 9(2)(a).
\textsuperscript{238} Id. art. 9(2)(b).
\textsuperscript{239} GDPR, supra note 7, art. 9(2)(c).
There is also an exception for non-profit bodies, such as trade unions or religious groups, processing data about their members or former members if appropriate safeguards are implemented. The personal data “manifestly made public by the data subject” is also excepted. The “establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity” is also excepted. Processing is also allowed “for reasons of substantial public interest, on the basis of Union or Member State law,” so long as the data is safeguarded. Processing is allowed for medicine diagnosis or for public health purposes. It is similarly allowed “for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,” so long as the data is secured.

C. Rights of the Data Subject

IoT controllers must provide transparent information that is both accessible and understandable. Controllers should provide data subjects with information about collected data so that “data subjects should be able to reply also electronically and express their own privacy choices.”

1. Transparency and the Exercise of Rights by Data Subjects

IoT controllers have the duty to “facilitate the exercise of data subject rights.” They must provide minimum disclosures to data subjects “within one month of receipt of the request.” Controllers must “provide information on action taken on a request . . . without undue delay and in any event within one month of receipt of the request.” They must present data “in a concise, transparent, intelligible and easily accessible form, using clear and plain language.” Additionally, controllers must provide information “to the data subject without undue delay and in any event within one month of receipt of the request.” “If the controller does not take action on the request of the data

240. Id. art. 9(2)(d).
241. Id. art. 9(2)(e).
242. Id. art. 9(2)(f).
243. GDPR, supra note 7, art. 9(2)(g).
244. Id. art. 9(2)(h)-(i).
245. Id. art. 9(2)(j).
246. Id. art. 11.
248. GDPR, supra note 7, art. 12(2).
249. Id. art. 12(3).
250. Id. art. 12(1).
251. Id. art. 12(3).
subject, the controller shall inform the data subject without delay [or within one month of receipt stating] the reasons for not taking action.\textsuperscript{253}

2. Mandatory Minimum Information Where Personal Data Is Collected

IoT manufacturers must provide “end-users with comprehensive information about their processed personal data - have resulted in significant workload as well as administrative challenges.”\textsuperscript{254} At the time data is collected, a controller must inform the data subject of “the identity and the contact details of the controller and, where applicable, of the controller’s representative.”\textsuperscript{255} Data controllers must disclose information on how to contact “the data protection officer where applicable.”\textsuperscript{256} Controllers must also disclose the purposes for processing a data subject’s personal data.\textsuperscript{257} They must inform the subject about “the legitimate interests pursued by the controller,” such as consent by the data subject and other Article 6 exceptions.\textsuperscript{258}

Controllers must disclose who are “the recipients . . . of the personal data, if any.”\textsuperscript{259} They must also disclose whether any adequacy decision exists as to any transfers of personal data to third countries or international organizations.\textsuperscript{260} Controllers must give data subjects any “reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.”\textsuperscript{261} They must also provide the data subject with the following further information necessary to ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
(d) the right to lodge a complaint with a supervisory authority;
(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as

\textsuperscript{253} Id.
\textsuperscript{254} See Herberger, supra note 195.
\textsuperscript{255} GDPR, supra note 7, art. 13(1)(a).
\textsuperscript{256} Id. art. 13(1)(b).
\textsuperscript{257} Id. art. 13(1)(c).
\textsuperscript{258} Id. art. 13(1)(d).
\textsuperscript{259} GDPR, supra note 7, art. 13(1)(e).
\textsuperscript{260} Id. art. 13(1)(f).
\textsuperscript{261} Id.
whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.²⁶²

3. Disclosures Where Data Is Not from the Data Subject

The GDPR requires a data controller to provide a data subject with certain information when the subject’s personal data was obtained through means other than the subject; such data includes:

(a) the identity and the contact details of the controller and, where applicable, of the controller’s representative;
(b) the contact details of the data protection officer, where applicable;
(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
(d) the categories of personal data concerned;
(e) the recipients or categories of recipients of the personal data, if any;
(f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organ[ization] and the existence or absence of an adequacy decision by the Commission.²⁶³

Controllers must also give data subjects “the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period.”²⁶⁴ The controller must inform the data subjects of their right to rectify or erase personal data, or their right to object to data processing.²⁶⁵ They also have a right to transfer data, which is the right of portability.²⁶⁶ IoT makers need to operationalize how they will provide information where personal data is collected from the data subject.²⁶⁷ Moreover, IoT makers will also need to show how they provide personal data to persons where they did not obtain it from them.²⁶⁸

²⁶²  Id. art. 13(2)(a)-(f).
²⁶³  GDPR, supra note 7, art. 14(1).
²⁶⁴  Id. art. 14(2).
²⁶⁵  Id. art. 14(2)(c).
²⁶⁶  Id.
²⁶⁷  GDPR, supra note 7, art. 13.
²⁶⁸  Id. art. 14.
4. Right of Access

The GDPR gives data subjects a right of access to their personal data.269 Controllers must give data subjects information about the purposes of the processing.270 The categories of personal data must also be disclosed.271 Data subjects disclose “particular recipients in third countries or international organ[i]zations,” the contemplated period for which the personal data will be stored, or, “if not possible, the criteria used to determine that period.”272 Controllers must give data subjects disclosures of their “right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.”273

5. Right to Rectification

The GDPR gives data subjects the right to get inaccurate data corrected or rectified.274 Consumers also have a right to have incomplete personal data completed; however, completion depends upon the purposes for the processing.275 This may involve providing a supplementary statement to the incomplete data to update or correct personal information.276

6. The Right to Be Forgotten

The Court of Justice of the European Union (CJEU) acknowledged a right to be forgotten in Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos.277 The court’s decision in Google Spain recognized the right of a Spanish attorney to have personal data about his insolvency delinked so this information would not appear in response to a search for his name in a search engine.278 In this high-profile case, the CJEU classified Google as a controller of personal data, making Google responsible for removal of the information.279 The CJEU’s recognition of the right to be forgotten under the DPD stems from the notion of privacy as a fundamental right.280

269. Id. art. 15.
270. Id. art. 15(1)(a).
271. GDPR, supra note 7, art. 15(1)(b).
272. Id. art. 15(1)(c)-(d).
273. Id. art. 15(1)(e).
274. Id. art. 16.
275. GDPR, supra note 7, art. 16.
276. Id.
279. Id.
280. Id. at 416.
After May 25, 2018, IoT controllers must explain to users how they store and process information, and provide a mechanism to delete or request deletion of information to comply with the GDPR’s right to be forgotten. A 2016 study found that IoT device makers were not transparent about their contact information or how they processed personal data, and that they failed to disclose how data subjects could exercise their right to erase personal data: “59% of IoT devices failed to explain to users how they process user data; 68% failed to explain how they store information; 72% failed to explain how to delete data; 38% failed to include contact information.”

The EU right to be forgotten can be conceptualized as taking three forms: the right to have information deleted after a preset period; the right to have a clean slate; and the right to be connected to current information and delinked from outdated information. EU data subjects have the right to “request the removal of links by search engines, who are data controllers. This right, now called the right to erasure, is a fundamental data subject right in the GDPR, in and beyond the context of publicly available personal information.” Article 17 provides that the data subject’s right to be forgotten and to erasure when “personal data are no longer necessary.” A data subject has the right to erase links to data relating to him or her if the information is:

[N]o longer necessary in relation to the purposes for which [it was] collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.

The right to be forgotten also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology blocking. The EU Commission’s Explanatory Memorandum makes a policy-based decision that the data controller, not the data subject, must notify third-party websites

281. Rights of Data Subjects Under GDPR, HIPAA J. (June 11, 2018), https://www.hipaajournal.com/rights-of-data-subjects-under-gdpr/ (explaining fundamental rights of data subjects under GDPR). “The right to erasure—also referred to as the right to deletion or the right to be forgotten—allows a data subject to stop all processing of their data and request their personal data be erased (Article 17).” Id.


284. The Right to Erasure or Right to be Forgotten Under the GDPR Explained and Visualized, i-SCOOP, https://www.i-scoop.eu/gdpr/right-erasure-right-forgotten-gdpr/ (indicating highly unacceptable lack of consent circumstances relating to IoT devices).

285. GDPR, supra note 7, art. 17(1).

286. Id. recital 65.

287. Id. art. 17(2).
when a data subject has requested it erase “any links to, or copy or replication of . . . personal data.” 288 The data controller is not required to comply with the data subject’s request to erase personal data if the subject of the data request falls into one of five exceptions.289

These exceptions are: the right of expression and information; compliance with a legal obligation; public interest or public health; public interest, science, or research; and establishing, exercising, or defending legal claims.290 De-indexing and removing personal data will lead to Internet censorship:

Nor does the EU right to be forgotten proposal distinguish between true or false information, so data subjects will also be able to suppress truthful information as long as the data does not fit within a statutory exception. This places the data controller in the unenviable position of effectively rewriting history. Furthermore, data controllers must make these decisions in a vacuum. The right of erasure, as articulated in the GDPR, does not impose a burden on data subjects to provide any factual foundation for their data request or even assert that the website posting or other information that is the basis for the request violates the law, defames, or humiliates. The consequence of the broad right of erasure is that Google and other data controllers are in the position of gatekeepers that determine which data erasure requests should be granted and which should be denied, without sufficient guidance.291

7. Right to Restrict Processing

Data subjects have a right to require controllers to restrict processing of their personal data, where they contest the accuracy of the personal data.292 Moreover, they may restrict the processing of their personal data where “the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead.”293 The controller must restrict personal data if the controller no longer needs it but the data subject needs “the data . . . for the establishment, exercise or defen[se] of legal claims.”294 Controller must restrict data where “the data subject has objected to processing . . . pending the verification whether the legitimate grounds of the controller override those of the data subject.”295 “A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the

288. See id.; European Commission Fact Sheet MEMO/15/3685, Questions and Answers—Data Protection Reform (Dec. 21, 2015).
289. GDPR, supra note 7, art. 17(3).
290. Id.
291. Rustad & Kulevska, supra note 278, at 369, 370.
292. GDPR, supra note 7, art. 18(1)(a).
293. Id. art. 18(1)(b).
294. Id. art. 18(1)(c).
295. Id. art. 18(1)(d).
controller before the restriction of processing is lifted.”296 It is unclear how IoT controllers can alert users about their rights to restrict their personal data.297

8. Controller’s Duty to Notify Rectification or Erasure of Personal Data

IoT controllers will also find it difficult to give data subjects notice of any correction or erasure of their processed data.298 Data subjects not only have a right of rectification and erasure, but a right to be notified when their personal data has been altered.299 IoT controllers subject to the GDPR need protocols for handling requests from data subjects for correcting or erasing personal data, as well as notifying the data subject of any changes.300

9. Data Transfer and Portability

The GDPR recognizes the data subject’s right to data portability (RTDP), which is the transfer of data from one electronic processing system to and into another.301 “Bringing the new [RTDP] from an abstract legal provision . . . into practice requires a greater role for the IT design community.”302 “Many IoT services maintain an ongoing relationship with users where their personal data is mined and analy[zed] with the goal of providing value added, contextually appropriate, services.”303 The RTDP includes both a right to receive personal data in a machine-readable format,304 and a right to transmit data from one controller to another.305

The GDPR gives data subjects the right “to have [their] personal data transmitted directly from one controller to another, where technically feasible.”306 As a precondition to further improve access to personal data, the GDPR also provides the right to obtain from the controller those data in a structured and commonly used electronic format.307
10. Measures Based on Profiling

Article 22, titled *Automated Individual Decision-Making, Including Profiling*, gives data subjects the “right not to be subject to a decision based solely on automated processing.”308 The opt-out right is not applicable to automatic processing “necessary for entering into, or performance of, a contract between the data subject and a data controller.”309 Similarly, data subjects have no right to opt out of processing mandated by law assuming the controller safeguards the data subjects’ rights and legitimate interests.310 Data subjects waive their right to object once they have explicitly consented.311 Article 22 posits exceptions to profiling based upon contract performance, express authorization by EU or Member State law, or a data subject’s consent.312

11. Restrictions on Data Subjects’ Rights

The GDPR gives the EU or Member States the right to place restrictions on obligations and rights of data protection to safeguard public security; the detection or prosecution of crimes; public interest of the EU or Member States; breaches of ethics of regulated professions; monitoring, inspection or regulatory functions of governmental agencies; and protection of the data subject and the freedoms of others.313 In addition, restrictions may be based upon the “investigation, detection and prosecution of breach of ethics for regulated professions.”314 Regulatory-connected restrictions, such as monitoring, inspections, or exercising official authority, are also legitimate restrictions on data subjects’ rights.315 Restrictions are also legitimated for protecting data subject protection and the freedom of others.316 Member States may restrict rights in order to enforce civil law claims.317

D. IoT Makers as Multiple and Co-Controllers

IoT product makers will also be classified as data controllers under the GDPR.318 The GDPR defines a “controller” to mean: persons that determine the

308. GDPR, supra note 7, art. 22(1).
309. Id. art. 22(2)(a).
310. Id. art. 22(2)(b).
311. Id. art. 22(2)(c).
312. GDPR, supra note 7, art. 22(2)(c).
313. Id. art. 23.
314. Id. art. 23(1)(g).
315. Id. art. 23(1)(h).
316. GDPR, supra note 7, art. 23(1)(i).
317. Id. art. 23(1)(j).
purposes of processing data. “As IoT involves multiple data controllers and co-controllers, with many layers of dependencies between different stakeholders to perform their duties required by the data protection and privacy laws. This may lead to confusion in terms of who is responsible and to what extent, leaving the data potentially vulnerable.”  A company “is a joint controller when together with one or more organi[zations] it jointly determines ‘why’ and ‘how’ personal data should be processed.” The GDPR adopts the “principle of accountability” and describes in detail the responsibility of the controller to demonstrate compliance, including by way of adoption of internal policies and mechanisms.

E. Data Privacy by Design and IoT Makers

Controllers have a duty to implement data protection by design and deal with risks as they arise. IoT applications must “consider security and privacy mechanisms early in their design phase, ensuring a configurable balance between reliability (requiring secure, trustworthy and precise data) and privacy (requiring data minimization)." The GDPR requires preventive law by protection by design and by default. “Accident prevention . . . is even better than accident compensation. . . . ‘A fence at the [t]op of the [c]liff [i]s [b]etter [t]han an [a]mbulance in the [v]alley [b]elow.’" IoT controllers will need preventive law measures that “address potential consumer data privacy and security concerns and implement security measures from the start, during the product development and design phase.”

Health product wearables must build privacy by design and must find a way of obtaining “consent (including in the high-growth market for connected
children’s products), identifying controllers and processors with IoT products, managing data transfers, and more.\(^{328}\) Articles 26 to 30 set forth the roles and duties of controllers and processors.\(^{329}\)

**F. Data Security and IoT Devices**

Insecure IoT devices “represent potentially efficient new ways of attack including the ease of surveillance practices, [and] data breaches resulting in personal data being stolen or compromised.”\(^{330}\) Many questions arise about unique vulnerabilities of IoT devices, “often deployed outside a traditional IT structure and lacking sufficient security built into them.”\(^{331}\) The “IoT raises several security challenges, namely as security and resource constraints force device manufacturers to balance battery efficiency and device security.”\(^{332}\) IoT makers have yet to balance “the implementation of confidentiality, integrity[, and] availability measures at all levels.”\(^{333}\) The WP29 Opinion noted that most IoT sensors on the market could not establish “an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.”\(^{334}\) The level of IoT security is only as good as its weakest component because “of the integration of physical and logical components provided by a set of different stakeholders.”\(^{335}\) The predominant risk is “that the IoT may turn an everyday object into a potential privacy and information security target while distributing those targets far more widely than the current version of the Internet.”\(^{336}\)

Security researchers have demonstrated the ability to take control of Internet-enabled cars through infotainment-like systems.\(^{337}\) White hat hackers proved that ransomware could be introduced into smart home thermostats.\(^{338}\) Ransomware-infected medical devices and “as many as 200,000 Windows systems, including those at forty-eight hospital trusts in the U.K. and so-far

---

329. GDPR, supra note 7, arts. 26-30.
331. Id. at 3.
332. Id. at 9.
333. Id.
335. Id.
336. Id.
unnamed medical facilities in the U.S.339 “[C]onnected and implanted medical devices—including cardiac pacemakers, drug administration devices, and monitoring devices, as well as infusion pumps, defibrillators, glucometers, and blood pressure measurement devices—can help patient care,” but create new risks.340

Hackers were able to “remotely unlock your smart lock if it relies on the Z-Wave wireless protocol.”341 Researchers uncovered “an attack that forces the current secure-pairing mechanism, known as S2, to an earlier version with known weaknesses, called S0.”342 The researchers demonstrated “the downgrade attack—dubbed Z-Shave—on a Conexis L1 Smart Door Lock from lock manufacture Yale. They note that an attacker within about 100 meters could, after the downgrade attack, then steal the keys to the smart lock.”343 The GDPR obliges the controller and the processor to implement appropriate measures for the security of processing.344 The problem is that many IoT makers have limited experience in implementing security.345 “As more and more smart devices are being used in the home, hackers will shift their focus from targeting individual devices, to hacking the apps that control networks of devices.”346 Researchers have uncovered vulnerabilities so that smart devices “could be controlled by the attacker—including a robot vacuum cleaner, refrigerators, ovens, dishwashers, washing machines and dryers, and air conditioners. Devices could be switched on and off, settings changed and more.”347

In 2016, “a botnet of an estimated 100,000 internet-connected devices were [sic] hijacked to flood the systems with unwanted requests and close down the Internet for millions of users.”348 “The malware, called Mirai scanned for [IoT]
devices that were still using their default passwords and then enslaved those devices into a botnet, which was then used to launch the attacks. The GDPR introduces the obligation of controllers and processors to carry out a data protection impact assessment prior to undertaking risky processing operations. Article 34 requires controllers or processors to seek authorization from the supervisory authority to ensure compliance with the GDPR. IoT makers who fail to implement reasonable security in their devices do so at their peril.

The most significant security weakness of the IoT is that it increases the number of hackable devices including “our car, our home appliances, our wearables, and many other IoT devices.” IoT makers do “not update their devices enough or at all. This means that an IoT device [that] was safe when you first bought can become unsafe as hackers discover new vulnerabilities.” IoT makers are classified as controllers; therefore, they have a duty to implement appropriate measures for processing security.

Every jurisdiction requires companies that experience a data breach to notify those consumers whose information has been compromised. The GDPR introduces an obligation to notify personal data breaches, strengthening the breach notification rules of the DPD. IoT makers need a mechanism to ensure prompt notification of a personal data breach to the supervisory authority and to the data subject.

The GDPR provides data controllers must notify the competent supervisory authority of a breach of security “without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach.” The controller must also document “any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.” The GDPR requires the controller to communicate a


349. Id.
350. GDPR, supra note 7, art. 33.
351. Id. art. 34.
353. Id.
354. GDPR, supra note 7, art. 32.
356. GDPR, supra note 7, art. 33.
357. Id. art. 33(1)
358. Id. art. 34.
359. Id. art. 33(1).
360. GDPR, supra note 7, art. 33(5).
personal data breach to the data subject. 361 The GDPR requires controllers or processors to seek authorization from the supervisory authority before undertaking risky processing activities. 362 IoT makers who fail to implement reasonable security in their devices do so at their peril.

G. Data Protection Impact Assessment and Authorization

The GDPR introduces the obligation of controllers and processors for new technologies to carry out a data protection impact assessment prior to undertaking risky processing operations. 363 The goal of the impact assessment is to assess and reduce the risks of protecting personal data. 364 The impact assessment must conduct “a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based.” 365 Impact assessments must also be completed if for “processing on a large scale of special categories of data . . . or of personal data relating to criminal convictions and offences.” 366 An audit is required for large scale “monitoring of a publicly accessible area.” 367 The GDPR requires controllers or processors to seek authorization from the supervisory authority to ensure compliance with EU data protection law where there is high risk processing. 368

The GDPR creates the role of the data protection officer who serves both the private and public sectors or for large enterprises, or where the core activities of the controller or processor consist of processing operations requiring regular and systematic monitoring. 369 Article 37 sets out the position of the data protection officer while Article 38 addresses the position of data protection officers. 370 IoT makers must appoint a data protection officer because they are controllers and the processing operations are continuous. 371 The GDPR addresses codes of conduct for data protection officers. 372 The GDPR recognizes certification mechanisms and data protection marks and seals. 373 The European Commission will provide technical standards for certification. 374

---

361. Id. art. 34(1).
362. Id. art. 34(4).
363. Id. art. 35(1).
364. GDPR, supra note 7, art. 35(1).
365. Id. art. 35(3)(a).
366. Id. art. 35(3)(b).
367. Id. art. 35(3)(c).
368. GDPR, supra note 7, art. 36.
369. Id. art. 37.
370. Id. art. 37-38.
371. Id. art. 37.
372. GDPR, supra note 7, art. 40.
373. Id. art. 42.
374. Id.
H. Transfers of Personal Data

Chapter 5 of the GDPR is entitled *Transfers of personal data to third countries or international organisations.* IoT controllers cannot transfer European consumer data to third countries unless they comply with the data processing obligations of the GDPR. These rules are mandatory for any transfers of “personal data to a third country or an international organ[ization],” including onward transfers. Article 46 sets out the criteria and procedures for when a controller or processor has the appropriate level of data protection safeguards. Article 45 sets out the criteria, conditions, and procedures for determining whether a receiving state has an adequate level of data protection. The GDPR requires the Commission to publish “a list of the third countries, territories and specified sectors within a third country and international organ[i]zations” for which it has decided an adequate level of protection is or is on longer ensured.

The GDPR states data controllers or processors—in the absence of a Commission decision—may not transfer data unless they determine the receiving state has implemented the appropriate safeguards such as Article 47’s binding corporate rules, or data protection clauses approved by the EU Commission or “adopted by a supervisory authority and approved by the Commission.”

IV. REMEDIES, LIABILITIES, AND SANCTIONS

A. Private Enforcement to Supplement Public Enforcement

Historically, privacy enforcement in Europe was performed exclusively by national public authorities. For the first time, the GDPR gives data subjects the right to file causes of action against supervisory authorities in the state of residence, place of employment, or where the infringement took place. The supervisory authority must inform the data subject of the status and outcome of the complaint including any available judicial remedy. Data subjects are entitled “to an effective judicial remedy against a legally binding decision of a supervisory authority concerning them,” and have recourse against supervisory authorities who do not handle complaints effectively or “within three months on the progress or outcome of the complaint.” Data subjects also have

375. *Id.* ch. 5.
376. GDPR, *supra* note 7, art. 45.
377. *Id.* art. 46(1).
378. *Id.*
379. *Id.* art. 45.
380. GDPR, *supra* note 7, art. 45(8).
381. *Id.* art. 46(2)(b)-(d).
382. *Id.* art. 77(1).
383. *Id.* art. 77(2).
384. GDPR, *supra* note 7, art. 78(1).
385. *Id.* art. 78(2).
a right to challenge “a legally binding decision of a supervisory authority.”

They have a right “to an effective judicial remedy where the supervisory authority . . . does not handle a complaint or does not inform the data subject within three months on the progress or outcome of” of a lodged complaint.

Data subjects additionally have the right to initiate proceedings “against a supervisory authority” in the courts in the EU country “where the supervisory authority is established.” The GDPR gives data subjects “the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation.” The data subject can file suit against the controller or processor in courts where they have a “habitual residence” where “unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.” Alternatively, they may sue controllers or processors in Member States where they have an establishment.

B. Representation Actions on Behalf of Data Subjects

Data subjects have a right to mandate a not-for-profit body, organization, or association to represent them to file a complaint on their behalf to protect their personal data. Member States may form “any body, organi[zation] or association” that can file representative actions to protect those whose privacy has been infringed “as a result of the processing.” The GDPR’s representation lawsuit is a functional equivalent of a class action, but filed by a nonprofit organization or association. The GDPR recognizes the right of data subjects to compensation for material or nonmaterial damage as a result of any GDPR infringement, and those subjects shall have the “right to receive compensation from the controller or processor” if they suffer damages from having their personal data compromised. “A processor shall be liable for the damage caused by processing only where it” violated the GDPR rules on processing data “or where it has acted outside or contrary to lawful instructions of the controller.”

Controllers or processors can defend against these claims if they can prove “that [they are] not in any way responsible for the event giving rise to the

386. Id. art. 78(1).
387. Id. art. 78(2).
388. GDPR, supra note 7, art. 78(3).
389. Id. art. 79(1).
390. Id. art. 79(2).
391. Id.
392. GDPR, supra note 7, art. 80(1).
393. Id. art. 80(2).
394. Id. art. 80(1).
395. Id. art. 82(1).
396. GDPR, supra note 7, art. 82(2).
The GDPR imposes joint and several liability against controllers or processors.398 “[E]ach controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.”399 Controllers or processors may seek indemnification from “other controllers or processors involved in the same processing” according to their fault.400

C. Aggravating and Mitigation Factors for Administrative Fines

The GDPR developed criteria for determining whether to impose fines and factors determining their size, including “the nature, gravity and duration of the infringement”401 The fine should also reflect whether the violation of the GDPR was intentional or a product of negligence.402 Administrative fines may be reduced to the extent that the controller or processor mitigated any damages suffered by data subjects.403 Administrative fines must also reflect the degree of responsibility of the controller or processor considering technical and organizational measures they implemented.404 Administrative fines may be increased if there were “relevant previous infringements by the controller or processor.”405

A controller or processor’s “degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement” is a mitigating factor.406 The size of fines also depends upon “the categories of personal data affected by the infringement.”407 Courts and tribunals can also consider “the manner in which the infringement became known to the supervisory authority . . . and if so to what extent,” the controller or processor gave proper notice of the infringement.408 A court may lower a fine if the controller or processor complied with an approved code of conduct or certification mechanism.409 Courts or other tribunals may reduce or increase the fine for “any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.”410 The total amount of a fine “shall
not exceed the amount specified for the gravest infringement” where a controller
or processor infringes several provisions of the GDPR.411

D. Bifurcated Schedule of GDPR Fines

The GDPR’s schedule of administrative fines is bifurcated depending upon
the nature of the offense. For obligations of the controller and the processor,
certification bodies, or monitoring bodies, fines are capped at ten million Euros,
“or in the case of an undertaking, up to 2% of the total worldwide annual turnover
of the preceding financial year, whichever is higher.”412 “This schedule applies
to “the obligations of the controller and the processor pursuant to [GDPR]
Articles 8, 11, 25 to 39 and 42 and 43.”413

Administrative are fines capped at twenty million euros and up to four percent
of the total worldwide annual turnover of the preceding financial year, whichever
is higher for the following infringements affecting:

(a) the basic principles for processing, including conditions for consent,
pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects’ rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an
international organ[ization] pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter [9];
(e) non-compliance with an order or a temporary or definitive limitation on
processing or the suspension of data flows by the supervisory authority pursuant
to Article 58(2) or failure to provide access in violation of Article 58(1).414

Article 84 requires Member States set down rules to ensure that implemented
fines are “effective, proportionate, and dissuasive.”415 Potential fines up to four
percent of annual revenue turnover as well as the cost of litigation and reputation
are a sufficient deterrent for even the largest IoT maker to review and modify its
products, processes, and systems to comply with the GDPR. For the first time in
EU history, the Commission has enacted a mixed private and public enforcement
model that teaches the IoT makers and others that infringing privacy does not
pay.

IoT makers that market their devices to EU consumers must be vigilant to
comply with the GDPR considered global data protection standard. The GDPR
applies to an IoT maker’s processing activities related to the offering of goods or

411. Id. art. 83(3).
412. GDPR, supra note 7, art. 83(4).
413. Id. art. 83(4)(a).
414. Id. art. 83(5).
415. Id. art. 84.
services to the EU consumer marketplace irrespective of where the IoT processer is physically storing the data. This Article has examined the specific duties of IoT makers in complying with the GDPR. The GDPR imposes large penalties against non-compliant IoT makers. Fines can be levied up to the greater of ten million euros or two percent of global gross turnover for violations of record keeping, security, breach notification, and privacy impact assessment obligations. These penalties may be doubled to twenty million euros or four percent of turnover for violations related to legal justification for processing, lack of consent, data subject rights, and cross-border data transfers.

V. CONCLUSION

The GDPR consists of ninety-nine articles. The key provisions of the GDPR for IoT manufacturers are: an expanded jurisdictional reach applied to non-European companies that process the data of European consumers; the duty to notify consumers of a data breach within twenty-four hours; the requirement for companies to obtain a “specific, informed[,] and explicit” consent before collecting personal data (the opt-in provision); and a company’s duty to erase personal data upon demand (the right to be forgotten). IoT makers need a comprehensive privacy and security audit to identify unique IoT threats while simultaneously implementing security to reduce these risks and complying with the stringent GDPR requirements for the processing of personal data irrespective of where they are organized, headquartered, or located.

IoT makers must either comply with the GDPR or cease doing business in Europe, one of the world’s largest trading blocks. IoT makers must conduct an impact audit of their privacy policies and procedures, train their employees to comply with the GDPR requirements, implement information security, and have a security breach response team in place to give notice to affected consumers within seventy-two hours. The IoT transcends national boundaries, and thus requires a radical rethinking of the nature of privacy compliance. IoT device makers with global ambitions need to globalize their legal audits to fulfill GDPR duties. A comprehensive audit must answer the following questions: (1) Does the individual know I am collecting the data? (2) How am I planning to use this data? (3) Does the individual know why I am collecting the data? (4) Is there a way of achieving this purpose without having to collect the data? (5) How long will I need the data to achieve the purpose?


IoT makers can first limit the radius of risk of GDPR compliance by incorporating pre-approved, standardized corporate clauses addressing privacy that are subject to approval by the European Commission and other supervisory authorities. IoT makers with global ambitions need to take inventory of how their IoT devices use personal data and communicate such use to customers. IoT makers do not have a roadmap on how to obtain consent to process their personal data. The largest challenge for IoT makers is to safeguard the data they process, and to develop a protocol to detect espionage and stave off cyberattacks. Another challenge is that IoT makers have only a seventy-two-hour window for reporting and responding to data breaches. Ideally, IoT would follow principles of privacy by design to achieve GDPR compliance. Finally, the IoT must operationalize the GDPR’s right to be forgotten, data portability rights, and the right to object to automated decision making. The GDPR will create a de facto worldwide data protection standard as IoT makers will find it more efficient to implement privacy by design in all of their devices, not just those found in Europe.