INFORMATION LAW JOURNAL

A Publication of the Information Security and EDDE Committees
ABA Section of Science & Technology Law

SPRING 2016 VOLUME 7 ISSUE 2 EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

The Internet-of-Things (IoT) (or Internet of Everything) – Privacy and Data Protection Issues in the EU and the US

By Francesca Giannoni-Crystal and Allyson Haynes Stuart

The Internet-of-Things (IoT) (or internet-of-everything as it is often interchangeably called) is officially "the next big thing." The growing proliferation of connected devices has far-reaching implications for consumer privacy and security at the same time that it promises to ease every-day life and increase health and safety. This year's Consumer Electronics Show (CES) featured everything from smart washing machines that will tell their owners when they need to buy detergent, *Read more*

Making Lemonade out of Lemons: The Cybersecurity Information Sharing Act of 2015

By Jason Edgecombe and Frederick Scholl

On December 18, 2015, President Obama signed the omnibus spending bill for the coming year. Inserted into the final bill was the Cybersecurity Information Sharing Act ("CISA") which, when fully implemented, is intended to create a process to allow the private sector and the federal government to share information concerning cybersecurity threats, distribute that information, and—ideally—inhibit the spread of such threats. That is the vision, at any rate. But questions still *Read more*

Biometric Collection: A New Era of Technology and Privacy Concerns

By Ashley L. Thomas

"If someone hacks your password, you can change it – as many times as you want. You can't change your fingerprints. You have only ten of them. And you leave them on everything you touch." Senator Al Franken. Companies are making concerted efforts to ramp up cybersecurity efforts but it appears that hackers are not always far behind overcoming those security efforts. In an effort to use alternative means of security, companies are turning to biometric identification to make *Read more*

EU's General Data Protection Regulation – What Does It Mean for Business?

By Kate Colleary

After many years of negotiation, consulting, drafting and even a movie made about it, on 15 December 2015, the European Parliament, Commission, and Council of Ministers reached agreement on the text of the General Data Protection Regulation ("GDPR"). This draft is likely to be formally adopted in spring 2016. There will then be a two-year period following which the GDPR will become directly applicable in all European Union ("EU") member states. The GDPR will replace the *Read more*

The New Year Brings Changes to Proportionality and Sanctions Rules

By Khadijah Robinson, Alexander Hastings, and Edward Rippey

E-discovery can be an extraordinarily expensive and time-consuming process, especially when preserving, collecting, and reviewing electronically stored information ("ESI"). In response to ongoing concerns regarding these burdens, the Advisory Committee on Rules of Civil Procedure (the "Committee") proposed several changes to the Federal Rules of Civil Procedure, which became effective on December 1, 2015. The two most significant amendments for e-discovery appear in *Read more*

A Hidden Insider Threat: Exposing Visual Hackers

By Mari J. Frank

When we think of hackers breaching systems and stealing information from our law firms or our clients' businesses, we don't usually suspect trusted employees as the guilty parties. But insider threats are in fact a very real and growing challenge. Security services provider SANS Institute surveyed nearly 800 IT and security professionals across multiple industries and found that 74 percent of respondents were concerned about negligent or malicious employees *Read more*

The Internet-of-Things (IoT) (or Internet of Everything) – Privacy and Data Protection Issues in the EU and the US

By Francesca Giannoni-Crystal and Allyson Haynes Stuart


The Internet-of-Things (IoT) (or internet-of-everything as it is often interchangeably called[1]*) is officially "the next big thing." The growing proliferation of connected devices has far-reaching implications for consumer privacy and security at the same time that it promises to ease every-day life and increase health and safety. This year's Consumer Electronics Show (CES) featured everything from smart washing machines that will tell their owners when they need to buy detergent*, to connected changing tables that will keep parents apprised of the weight of their babies' dirty diapers.[2] The age of smart homes is upon us, with alarm systems, air conditioning units, keyless entries and sprinkler systems all talking to each other – and to their owners.

At present, the news is more technological than legal. Nonetheless, the IoT triggers some worrisome legal issues, including: data collection, data security, invasion of privacy, bandwidth, and copyright.[3] The issues are imposing because of the potential magnitude of the phenomenon. Very little explicit regulation on the IoT exists and there is confusion about which existing laws should apply to the IoT. Since the IoT is likely to grow exponentially in the next few years,[4] these legal issues should be tackled

---

[1] We will use the two terms as synonyms, according to the general usage, however, according to some experts, "Internet-of-Things" and "Internet-of-everything" are not the same thing. In her blog reporting on the annual conference of Cisco held in San Francisco in 2014 – Noelle Knell explains the difference between the two concepts. Reporting the statements of CISCO's Internet of Things Vice President Tony Shakib, the distinction of the two concepts is drawn as follows:

> The internet of things … is simply the connectivity – the infrastructure that is established in order for Internet-connected devices to interoperate, while "[t]he internet of Everything … involves three additional components. The second component is the data that is generated by connecting such a vast web of things … The third piece is the smart applications used to solve public-sector problems, or the management layer. The final piece is the application enablement. … All four layers together are the Internet of Everything" Noelle Knell, *Cisco Live: Internet of Things vs. Internet of Everything*, http://www.govtech.com/network/Cisco-Live-Internet-of-Things-vs-Internet-of-Everything.html.

Based on this specification, because this article does not deal with connectivity issues, but with privacy issues, it would probably be more correct to talk about "Internet-of-Everything" but we give in to the buzzword and we do not draw a distinction.

[2] Roger Cheng, *Oh poop. Baby tech rattles a dad to be*, CNET (Jan. 10, 2016), http://www.cnet.com/news/oh-poop-baby-tech-rattles-a-dad-to-be/.

[3] See Brian Wassom, *Top 5 Legal Issues in the Internet of Things, Part 1: Data Security & Privacy* (http://www.wassom.com/top-5-legal-issues-internet-things-part-1-data-security-privacy.html), *Part 2: Data Collection and Invasion of Privacy* (http://www.wassom.com/top-5-legal-issues-internet-things-part-2-data-collection-invasion-privacy.html) *Part 3: Bandwidth* (http://www.wassom.com/top-5-legal-issues-internet-things-part-3-bandwidth.html); *Part 4: Copyright* (http://www.wassom.com/top-5-legal-issues-internet-things-part-4-copyright.html); *Part 5: Physical Safety* (http://www.wassom.com/top-5-legal-issues-in-the-internet-of-things-part-5-physical-safety.html).

[4] Brain Wassom, *Top 5 Legal Issues in the Internet of Things, Part 5* (*supra* note 3):

now.[5] This is particularly true for the two legal issues on which we will focus in this article: privacy and data protection.

I. The IoT: A Definitional Problem

The first problem we encountered with the IoT is definitional.[6] In fact, there is no set definition of the IoT.

We might define the IoT as "a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction."[7] A "unique identifier" refers to a "numeric or alphanumeric string that is associated with a single entity within a given system."[8]

The FTC, in its report on the IoT,[9] uses a less technological definition: the IoT refers "to 'things' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet."[10]

The Article 29 Data Protection Working Party ("WP29")[11] defines the IoT as the "infrastructure in

---

> That would be as pointless as arguing against the tides; they will arrive regardless of anyone's opinion. But there is plenty of room for foresight and advance planning, to ensure that the network of devices that already exists and that grows more complex every day is built in an intentional, prudent manner that maximizes its utility to society and minimizes its dangers.

[5] As IoT products continue to connect more and more aspects of our lives, it means more and more of our private information is being entrusted into the hands of IoT companies. In 2016, IoT companies will be forced to increase security features to ensure users' private information is safer than ever before.
Chris Klein, *2016 predictions for IoT and smart homes*, http://thenextweb.com/insider/2015/12/23/2016-predictions-for-iot-and-smart-homes/#gref.

[6] Roberto Minerva, Abyi Biru, Domenico Rotondi, *Towards a definition of the Internet of Things (IoT)*, issued by IEEE Internet Initiative, iot.ieee.org, http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf.

[7] Margeret Rouse, *Definition, Internet of Things (IoT),* http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[8] Margeret Rouse, Definition, Unique identifier (UID), http://internetofthingsagenda.techtarget.com/definition/unique-identifier-UID.

[9] On January 27, 2015, the Federal Trade Commission released a detailed report on the IoT, recommending a series of concrete steps for businesses to enhance and protect consumers' privacy and security. *Internet of Things. Privacy & Security in a Connected World* ("*FTC Report*"), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
"Although the term "Internet of Things" first appeared in the literature in 2005, there is still no widely accepted definition." FTC Report at 5.
See more on FTC's Report at http://www.technethics.com/ftc-provides-recommendations-to-address-iot-privacy-and-security-challenges/.

[10] FTC Report at 6.

[11] Article 29 Data Protection Working Party is a group -- set up under Article 29 of the Directive 95/46/EC - whose main task is providing expert opinion from the member state level to the Commission on questions of data protection. It consists of a representative of each country's DPA designed by each EU member state, one representative of the EU Commission and one representative from the other EU institution and bodies. See more at http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

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."[12] The WP29 identified the IoT with the principle of "extensive processing of data through … sensors."[13] Because these sensors communicate unobtrusively and with a "seamless" exchange of data,[14] the WP29 characterizes the IoT as pervasive and "ubiquitous computing."[15]

The same kind of difficulty of definition exists for similar concepts such as "machine to machine (M2M) communication."[16] To be sure, M2M and IoT are not the same thing, even if many use these two terms interchangeably. The problem is that there is no agreement on what the difference is. For some the IoT is a broader term and includes M2M; [17] for others the difference is in the way in which they achieve the remote access.[18] Other experts trace the difference in other ways: for example, the IoT would be a wider term because "IoT goes beyond M2M… beyond computers connecting to things. IoT represents things connecting with systems, people and other things."[19]

We raise this definitional issue not with the ambition of giving a definite answer to it or to the difference between IoT and M2M. Our purpose is simply to highlight another facet of the IoT problem. To be able to identify legal issues, one should be able to define the area in which the problems exist. If there is no clarity on what we are talking about, the task of identifying the underlying legal issues becomes almost impossible. Moreover, if there are to be special regulations regarding the IoT, we need to be able to define the field in which those regulations apply.

The difficulty in defining the phenomenon might be one of the reasons why the IoT has been much talked about but not much regulated: it is not easy to regulate something that cannot be easily defined. However, regulatory efforts on both sides of the Atlantic are in the works. EU legislation on IoT may be

---

[12] Opinion 8/2014 on the on Recent Developments on the Internet of Things, adopted on 16 September 2014 ("*Opinion on IoT*"), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf at 4.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] "Machine-to-Machine (M2M) communications is the communication between two or more entities that do not necessarily need any direct human intervention. M2M services intend to automate decision and communication processes." *Id.* at 12.

[17] *What is the difference between M2M and IoT?* Published by Telefónica m2m Tea, https://m2m.telefonica.com/blog/what-is-the-difference-between-m2m-and-iot.

[18] Chantal Polsonetti, *Know the Difference Between IoT and M2M*, http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m:

> [T]hey differ in how they achieve remote device access. For example, traditional M2M solutions typically rely on point-to-point communications using embedded hardware modules and either cellular or wired networks. In contrast, IoT solutions rely on IP-based networks to interface device data to a cloud or middleware platform.

[19] Bill Zujewski, *IoT vs. M2M... There's a Difference*, http://blog.axeda.com/archived-Axeda-blog-/tabid/90718/bid/104683/IoT-vs-M2M-There-s-a-Difference.aspx.

in the pipeline for 2016.[20] On the American side of the Atlantic, the California legislature has recently enacted Assembly Bill 1116,[21] which takes into account an increasing presence of smart TVs in our home.

II. General privacy and data protection issues in the IoT

According to a pessimistic view the IoT raises such imposing privacy issues that in an IoT environment, privacy would be simply "indefensible."[22] However, for scholars and regulators resignation is unacceptable. How can the daunting issues of privacy and data protection be addressed in this new environment?

First is the issue of privacy. Many of the new devices feature cameras, such as those in baby monitors. The cameras record activity and store it for the consumers. But who else may have access to those images? Recently, a story broke about a website that allows users to search for webcam images of sleeping babies.[23] Google Glass, one of the first "wearables," was criticized because it allows surreptitious pictures to be taken and uploaded on the Internet – even from a restroom.[24] All of the devices generate data, and with the collection of data come privacy issues of access to the data and appropriate use.

In addition to pictures or video feed that may contain private images, connected devices are beginning to include voice recognition features. Televisions, cars, even baby dolls are beginning to use voice recognition and often record their users. This raises the issue of unintentional recording of private conversations, or use of recordings for the wrong purpose.

Second and often overlapping is the issue of security. Just as it violates a person's sense of privacy to see video images of their home splashed on the Internet, it raises serious issues of security for strangers to have access to details of the home's interior layout and valuables alongside possible details of the owner's address and daily schedule. Even more scary is the possibility of hacking – a

---

[20] In November 2015, in a discussion on IoT policies, Mr. Kleiner (head at the European Commission Directorate General for Communications Networks, Content & Technology, DG Connect), said this is for the EU "key moment in policy in relation to IoT." Kleiner questioned whether the IoT should be addressed with a specific piece of legislation, or whether it would be sufficient to add elements to legislative plans already in the pipeline, like for example the Digital Single Market (DSM). He expects a decision on the best approach to regulate IoT by early 2016, and a document – probably in the form of a communication – to be issued by summer 2016. According to Kleiner, the Commission will look into the following key areas: free flow of data, standardization, data protection, telecommunications, and authentication of objects. *See* http://www.technethics.com/new-eu-legislation-on-iot-may-be-in-the-pipeline-for-2016/.

[21] CA Assembly Bill 1116, available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1116.

[22] *See* opinion expressed by NIST fellow Ron Ross and Robert Bigman, former chief information security officer at the CIA, as reported in the article of Sean Lyngaas, *NIST official: Internet of Things is "indefensible"*), https://fcw.com/articles/2015/04/16/iot-is-indefensible.aspx

[23] J.M. Porup, *How to search the Internet of Things for photos of sleeping babies*, Ars Technica (Jan. 19, 2016), http://arstechnica.co.uk/security/2016/01/how-to-search-the-internet-of-things-for-photos-of-sleeping-babies/.

[24] Nick Bilton, *At Google Conference, Cameras Even in the Bathroom*, The New York Times (May 17, 2013), http://bits.blogs.nytimes.com/2013/05/17/at-google-conference-even-cameras-in-the-bathroom/.

person obtaining access to the alarm system and disabling it at will, or taking over the controls of a car. This type of data breach is much higher risk than the common retail data breach, with a relatively small impact on end users.[25] In contrast, an IoT data breach, can have serious effects on end users, whose sensitive data is interconnected with personal devices, such as their door locks, cars, baby monitors, thermostats, lights, security cameras and other household appliances.[26] Data breaches have already affected internet-connected toys[27] and cars.[28]

Many other IoT devices have been found to have vulnerabilities making them susceptible to hacking. Fisher-Price's Smart Teddy Bear was found to have a bug that could allow children's identities to be exposed.[29] Toy Talk Barbie contained vulnerabilities that could allow hackers to spy on children's conversations.[30] The HereO watch and its accompanying iPhone and Android apps allow family members to track each other, but due to a bug in the application's platform web service, the HereO allowed potential hackers to pretend to be part of the family, "and thus gave stalkers a way to easily track and even send messages to any kids or family members wearing the watch."[31]

Some IoT devices are connected to publicly available webcams, a fact that is exploited by the company Shodan, whose search engine allows users to access publicly available webcams and still images – like those from baby monitors – from all over the world.[32] Also problematic are regular "glitches," such as a bug that caused Nest thermostats to stop working, errors in Fitbit's heart-rate monitoring, and malfunctioning door touch pads locking users out of their homes.[33]

Third is the issue of data protection (i.e. the organization and control of the processing of personal data), which technically is distinct from both privacy and cybersecurity, even if it is often used as a

---

[25] *See* Olivia Eckerson, *FBI CISO warns of IoT data breaches* (Sep. 23, 2015), http://internetofthingsagenda.techtarget.com/news/4500254067/FBI-CISO-warns-of-IoT-data-breaches.
[26] *Id.*
[27] Daniel Victor, *Security Breach at Toy Maker VTech Includes Data on Children*, The New York Times (Nov. 30, 2015), http://www.nytimes.com/2015/12/01/business/security-breach-at-toy-maker-vtech-includes-data-on-children.html.
[28] *See* John Villasenor, *Five Lessons on the 'Security of Things' from the Jeep Cherokee Hack*, Forbes (July 27, 2015), http://www.forbes.com/sites/johnvillasenor/2015/07/27/five-lessons-on-the-security-of-things-from-the-jeep-cherokee-hack/#3e4f8190204a.
[29] Lorenzo Franceschi-Bicchierai, *Internet-Connected Fisher Price Teddy Bear Left Kids' Identities Exposed*, Motherboard (Feb. 2, 2016), http://motherboard.vice.com/read/internet-connected-fisher-price-teddy-bear-left-kids-identities-exposed.
[30] Lorenzo Franceschi-Bicchierai, *Bugs in 'Hello Barbie' Could Have Let Hackers Spy on Childrens' Chats*, Motherboard (Dec. 4, 2015), https://motherboard.vice.com/read/bugs-in-hello-barbie-could-have-let-hackers-spy-on-kids-chats.
[31] Lorenzo Franceschi-Bicchierai, *A GPS Tracker for Kids Had a Bug that Would Let Hackers Stalk Them*, Motherboard (Feb. 2, 2016), https://motherboard.vice.com/read/a-gps-tracker-for-kids-had-a-bug-that-would-let-hackers-stalk-them?trk_source=recommended.
[32] Harriet Taylor, *Spying Through Strangers' Webcams Just Got Easier*, CNBC (Jan. 28, 2016), http://www.cnbc.com/2016/01/28/spying-through-strangers-webcams-just-got-easier.html.
[33] Nick Bilton, *Nest Thermostat Leaves Users in the Cold*, The New York Times (Jan. 13, 2016), http://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html?action=click&contentCollection=style&module=NextInCollection&region=Footer&pgtype=article&version=column&rref=collection%2Fcolumn%2Fdisruptions.

synonym of privacy.[34] This is eminently a European issue and we discuss it in Part III.

III. European Data Protection issues raised by the IoT

A. General data protection principles

There is no doubt that the IoT - at least until regulated by special legislation - is subject to the general EU data protection law. Today it means that it is subject to Directive 95/46/EC ("Directive")[35] and its national implementations. In the near future, it will be subject to the General Data Protection Regulation ("GDPR"),[36] expected to be formalized soon, to enter into force in 2018,[37] and to substitute for the Directive.

The Directive provides that it applies to the "to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system."[38] The term "processing" means "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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."[39] By "personal data", the EU law means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[40] Nobody could seriously contend that the IoT does not involve the "processing of personal data" as above defined. The GDPR's definition of "processing"[41] and "personal data"[42] will not

---

[34] DLA Piper, EU Study - Legal Analysis of a Single Market for the Informational Society, New Rules for a New Age? A. The Future of Online privacy and Data Protection, ec.europa.eu/newsroom/dae/document.cfm?doc_id=842
See, e.g., on the distinction between privacy and data protection, Nathan Crystal & Francesca Giannoni-Crystal, *Something's Got to Give - Cloud Computing, as Applied to Lawyers – Comparative Approach Us and EU and Practical Proposals to Overcome Differences*, Opinio Juris in Comparatione Vol.I, n.I, 2014, http://www.opiniojurisincomparatione.org/ at 35-35.

[35] 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[36] Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). While the GDPR is still not officially published, the Coreper released an unofficial text of the Regulation on January 28, 2016, http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/en/pdf. References to the GDPR in this Article reflect numbering in the draft released by Coreper on January 28, 2016. In the final version the numbering of the articles is likely to change.

[37] *See* http://www.technethics.com/european-data-protection-reform-council-confirms-agreement-with-the-european-parliament/ and here: http://www.technethics.com/eu-finds-agreement-on-data-protection-reform-formalization-in-early-2016-and-entering-into-effect-in-2018/.

[38] Directive, Article 3.

[39] Directive, Article 2(d) (emphasis added).

[40] Directive, Article 2(a) (emphasis added).

[41] GDPR, Article 4.3.

affect the conclusion that the general EU data protection will control the IoT. In addition, because the GDPR is regulation and not a directive, national laws of implementation will not apply anymore.[43]

The most important document about the application of EU data protection and IoT is Opinion 8/2014 on the Recent Developments on the Internet of Things,[44] an opinion of the WP29.[45] Our Paper relies heavily on this document because it spells out in detail the main privacy issues of the IoT under a European perspective and applies the current Directive to the IoT. The Opinion will still be of interest under the GDPR too because, while issued under the Directive, the WP29 already had the benefit of a draft of the new GDPR (the Commission's proposal was in January 2012), and the WP29 used the draft by crafting the Opinion with reference to the general principles of the GDPR. In particular, the Opinion uses the concepts of a wider scope of application of EU data protection law, privacy impact statements, security by design, portability, and others.[46]

The WP29's reliance on a draft proposal of the GPDR in preparing the Opinion on the IoT is quite evident in the discussion of the scope of application of the EU data protection law. The scope of the Directive is based on territoriality: the controller either has an establishment or uses equipment located in a Member state.[47] On the other hand, the GPDR uses a broader concept of "targeting" in determining the scope of its application.[48] While the WP29 Opinion refers to the articles of the Directive,[49] it contains a broad definition of "equipment" that makes its scope similar to the targeting concept of the GPDR.[50]

---

[42] GDPR, Article 4.1.The GDPR expands slightly on the Directive's definition of *personal data*. The Regulation now includes:

> any information relating to an identified or identifiable natural person 'data subject'; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. *Id.*

[43] "We notice that among the benefits of the future Data Protection Regulation is the fact that because it will be a 'regulation' and not a 'directive', it will provide a uniform privacy regulation in the 28 member states, unlike the present situation where individual state variations exist." *See* Nathan Crystal & Francesca Giannoni-Crystal, *Something's Got to Give - Cloud Computing, as Applied to Lawyers – Comparative Approach Us and EU and Practical Proposals to Overcome Differences*, *supra* note 35, at 39.

[44] *Supra* note 11.

[45] *See supra* note 10.

[46] *See* Korolyn Rouhani-Arani, *The Internet of Things and privacy in Europe and the USA*, available at http://united-kingdom.taylorwessing.com/globaldatahub/article_wp29_iot.html.

[47] Directive, Article 4.

[48] GDPR, Article 3.

> 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 behaviour as far as their behaviour takes place within the European Union.

[49] Opinion on IoT at 10.

[50] Opinion on IoT at 10. The WP29 has recently issued a new opinion on interpretation of Article 4 of the Directive. *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain*,

This (highly technical) Opinion is focused on three particular types of IoT (Wearable Computing, Quantified Self, and domotics)[51] but the Opinion can actually apply "outside its strict scope and cover … other developments in the IoT"[52] such as smart cities, smart transportations, and M2M.

B. Privacy challenges in the IoT

The WP29 recognizes the benefits of the IoT but also warns against privacy risks.[53] In particular, WP29 identified the following privacy challenges in IoT:

1. Lack of control and information asymmetry. IoT, with its pervasive and "unobtrusive" presence, might cause data subjects to lose control under several perspectives and result basically in a "third-party monitoring."[54] For this new situation, the WP29 warns that the usual tools of protection might not be appropriate. For example, the IoT collects data continuously, which makes it hardly possible for data subjects to review it before publication.[55] Also, because connected things communicate automatically and/or "by default," without individuals being aware of the connection,[56] users cannot effectively control "how objects interact"[57] and cannot "define virtual boundaries by defining active or non-active zones for specific things."

If users' control on data collection is hard, it is even harder for users to control the subsequent use of collected data,[58] which is obvious considering that users do not know exactly which data the "thing" collected. The risk of users' lack of control is enhanced when IoT, big data, and cloud computing are combined.[59]

---

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf. The broader interpretation of Article 4 of the Directive is confirmed in light of the CJEU judgement of 13 May 2014 in case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ("Google Spain"). See more on this Opinion at http://www.technethics.com/wp29-issues-new-opinion-on-law-applicable-in-light-of-the-cjeu-judgement-in-google-spain/.

[51] "Wearable Computing refers to everyday objects and clothes, such as watches and glasses, in which sensors were included to extend their functionalities… Quantified Self things are designed to be regularly carried by individuals who want to record information about their own habits and lifestyles". *Id.* at 5. "Domotics" refer to connected objects to automate home. *Id*. at 6.

[52] *Id.* at 5.

[53] *Id.*

> The Internet of Things (IoT) is on the threshold of integration into the lives of European citizens. ... [The] expected benefits must also respect the many privacy and security challenges which can be associated with the IoT… Thus, this opinion identifies the main data protection risks that lie within the ecosystem of the IoT before providing guidance on how the EU legal framework should be applied in this context. *Id.*

[54] *Id.* at 6.

[55] *Id.*

[56] *Id.*

[57] *Id*.

[58] *Id.*

[59] *Id*. at 7.

2. Quality of the user's consent. EU general data protection law requires consent for the legitimate processing of personal data (save exceptions).[60] Consent is a major problem with the IoT. Why? Because oftentimes users are not aware that a specific object is collecting their data, [61] which obviously makes controllers' reliance on data subjects' consent ungrounded. Indeed, how can they demonstrate that data subjects provided valid and "informed" consent (which is necessary under EU law, save exceptions),[62] when those data subjects did not know their data were being collected?[63] Some IoT objects, like smart watches, cannot be distinguished from the ordinary ones (example normal watch);[64] those devices are particularly insidious and they should be constructed to signal or warn people who may be "viewed" by such a device (example: through "signposting" on the object).[65]

Another problem with consent is that often the possibility to decline certain services or features of an IoT device is more theoretical than real, so the concept of free (and therefore valid) consent to processing is illusory.[66] In addition, the classical mechanisms to obtain consent are often inapplicable to the IoT: those mechanisms either generate what the WP29 calls a "low-quality" consent (low quality because it is based on a "lack of information")[67] or results in an impossibility for users to provide a "fine-tuned consent," in line with their preferences.[68] The solution, according to the WP29, is for the IoT stakeholders to implement new methods for obtaining valid consent; the WP29 mentions "privacy proxies" and "sticky policies" as possible methods.[69]

3. Inferences derived from data and repurposing of original processing. WP29 identifies a major privacy risk from the IoT in the "repurposing" of data:

The increase of the amount of data generated by the IoT in combination with modern techniques related to data analysis and cross-matching may lend this data to secondary uses, whether related or not to the purpose assigned to the original processing.[70]

The problem is that the data collected by a specific device might be insignificant (the WP29 refers to the accelerometer and the gyroscope of a smartphone as examples), but this raw information might

---

[60] Directive, Article 7. GDPR, Article 6. See more on this point at *Article 7 (legitimate data processing).*
[61] *Id.*
[62] *Id.* at 7.
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] Supported by a device, data requests are confronted with predefined policies governing access to data under the control of the data subject. By defining sensor and policy pairs, third parties requests for collection or access to sensor data would be authorised, limited or simply rejected. *Id.* note 30.
[70] *Id.* at 7.

allow the controller to "infer" much more significant information (for example, driving habits).[71] The IoT stakeholders must assure data subjects of consistency between the original purpose and the new purpose of the collection and must confirm that data subjects are aware of the new purpose.[72]

4. Intrusive bringing out of behavior patterns and profiling. The risk from the IoT is even greater than repurposing. Data collected by IoT devices can be "cross-matched" and might transform the IoT into a ubiquitous instrument of surveillance of individuals (both in public spaces and in their homes).[73]

What is "cross-matching" and why it is dangerous? Due to the "proliferation of sensors," a vast amount of separate (and perhaps insignificant) pieces of information will be collected and continuously cross-matched with one another. This mechanism will "reveal specific aspects of individual's habits, behaviours and preferences."[74] As a result, IoT stakeholders will be able to create general profiles of users, which is bad in itself. In addition, the continuous monitoring may influence the behavior of individuals because users, consciously or unconsciously, may change their behavior to comply with perceived norms.[75]

5. Limitations on the possibility to remain anonymous when using services. The complete development of IoT also means reduced possibilities for individuals to use services anonymously and to remain "unnoticed."[76] The reason is simple: think of wearable devices (such smart watches), which are used in close proximity to the data subject so that they are able to collect " identifiers" (such as the MAC addresses of other devices) that can track the location of users.[77] With the IoT everyone is traceable and "remaining anonymous and preserving one's privacy in the IoT will become increasingly difficult."[78]

6. Security risks. Security is one of the biggest concerns of the IoT for several reasons: *First*, at least for now device manufacturers prefer battery efficiency over security.[79] *Second*, because everyday objects will have sensors and will be connected with one another, the number of "security targets" will dramatically increase. The increase in connected devices will create an environment of reduced

---

[71] *Id.* at 7. The WP29 notes for example "how much information can be inferred from motion sensors though aggregation and advanced analysis" (type of "Quantified Self"): sensors capture "raw data (*e.g.*, data-subject motions) and rely on sophisticated algorithms to extract sensible information (*e.g.*, the number of steps) and deduce potentially sensitive information that will be displayed to the end users (*e.g.*, his physical condition)." The IoT stakeholder must ensure that "at each level (whether raw, extracted or displayed data) … 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." *Id.* at 7-8.
[72] *Id.* at 8.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.* at 8.
[77] *Id.*
[78] *Id.* at 9.
[79] *Id.* In particular, it is not yet clear how device manufacturers will balance the implementation of confidentiality, integrity and availability measures at all levels of the processing sequence with the need to optimise the use of computational resources – and energy – by objects and sensors. *Id.*

security because of the greater amount of surveillance and the likelihood of more data breaches (both data theft and tampering).[80] *Third*, cybersecurity must become multilevel: it is not enough to secure the devices; the IoT stakeholders must also secure "the communication links, storage infrastructure" and the entire IoT "ecosystem," as the WP29 expresses it. [81] *Fourth*, because more than one IoT stakeholder is expected to play a role in providing IoT services, cybersecurity will also have to include "adequate coordination" to avoid "weak points."[82]

C. Relevant data protection principles

In dealing with these privacy challenges, the WP29 has clarified[83] that the IoT is subject to the framework of the general Data Protection Directive 95/46/EC (and the national implementation therefore) and of the Data Protection in the Electronic Communications Sector Directive 2002/58/EC[84] (as amended by Directive 2009/136/EC).[85] While often the application of the Directives may be difficult (because the data are not provided by users but are collected by sensors and also for the other reasons discussed above as privacy challenges), the WP29 has not exempted the IoT from the application of any of the general data protection rules.

The WP29 has made clear that data originating from things is often "personal data" (therefore subject to the general data protection) pursuant to Article 2(a) of Directive 95/46/EC because individuals are likely to be identified from that data.[86] The WP29 warns that this is the case also even when pseudonymisation or anonymisation techniques are used because "the large amount of data processed automatically in the context of IoT entails risks of re-identification."[87] Consider that, in the IoT environment the data subjects that must be protected are not only the subscribers of an IoT service or the users of a device but also individuals that are neither subscribers nor users. This is the case for example for wearables (such as smart glasses), which are capable of collecting data from data subjects other than "the owner of the device."[88]

The WP29 concludes that at least the following provisions of Directive 95/46/EC come into play with IoT:

---

[80] *Id.*
[81] *Id.*
[82] *Id.* The WP29 highlights that, for example, "most of the sensors currently present on the market are not capable of establishing an encrypted link for communications." *Id.*
[83] *Id.* at 10.
[84] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32002L0058.
[85] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF.
[86] Opinion on IoT at 10.
[87] *Id.* at 11.
[88] *Id.* at 13.

- *Article 7 (legitimate data processing).*[89] If IoT stakeholders are data controllers (*i.e.*, they determine "the purposes and means of the processing of personal data" in the meaning of Article 2(d) of the Directive), they must comply with one of the alternative requirements of Article 7.[90] The main avenue for a legitimate data processing is data subject consent. Article 7(a). The consent must have the characteristics specified by WP29's Opinion 15/2011.[91] Article 7 provides also alternatives to consent, the main of which is when the processing is "necessary for the performance of a contract to which the data subject is party." Article 7(b). The WP29 notes that the link between the processing and the performance of the contract must be "direct and objective,"[92] *i.e.*, the contract cannot be a pretext for processing the data. Consent is not required when processing is necessary to comply with a legal obligation of the controller (Article 7(c)) or to protect the "vital interest" of the data subject (Article 7(d)) or to perform a task carried out "in the public interest" (but the controller must have an official authority or must disclose data to someone with official authority). Article 7(e). The most controversial case of lawful processing without consent is listed in subsection (f) of Article 7 and is based on the "legitimate interests" of the controller or third parties. The interpretation of this exception to consent is quite narrow, and the "legitimate interests" can never trump the fundamental rights of the data subject (*in primis* the right of privacy).[93] It is very difficult (for a IoT stakeholder or any other controller) to rely on this exception to consent, and the more sensitive the information, the more difficult it is to pass muster.[94]

- *Article 6 (fair and lawful data collection and processing)*.[95] The data processing in the IoT environment must respect the "fair and lawful" collection/processing principle and the "minimization" principle,[96]

---

[89] Opinion on IoT at 14-16. The "Lawfulness of processing" is in Article 6 of the new Regulation.

[90] *Id.* at 15. The WP29 specifies that "[t]hese requirements apply to some of these stakeholders on top of the application of Article 5(3), when the processing at stake goes beyond the storage of, or the gaining access to information stored in the user/subscriber's terminal equipment." *Id.*

[91] *Opinion 15/2011 on the Definition of Consent*, adopted on 3 July 2011 (WP187), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[92] Opinion on IoT at 15.

[93] The European Court of Justice has interpreted this exception, among others, in Judgment of the court (Grand Chamber), 13 May 2014, Case C-131/12 (paragraphs 74 ff.) (the Google case). We note *in passim* that European countries generally do not see a request for pretrial discovery from the US as a "legitimate interest" (see, e.g., Hughes Hubbard & Reed LLP, *The Impact on U.S. Discovery of EU Data Protection and Discovery Blocking Statutes*, http://www.hugheshubbard.com/Documents/Impact_on_U_S_Discovery_of_EU_Data_Protection_and_Discovery_Blocking_Statutes.pdf). The limitation of this exception to consent is clearly spelled out in the GDPR, which specifies that legitimate interests are not a basis for a consentless processing when "such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." Article 6(f).

[94] *Id.*

[95] *Id.* at 16-17.

[96] The WP29 opines that, unlike what some players think, the minimization principle is not "a barrier for innovation." *Id.* We note incidentally that the "minimization principle" is not an expression of the Directive; instead, the expression comes from Article 5.1(c) of the GDPR (this is another example of the WP29's using the GDPR's terminology even if not yet in force): "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')."

which together constitute the "cornerstone" [97]– as the WP29 expressed it – of EU data protection law. Personal data must be "processed fairly and lawfully" (Article 6.1(a)) and must be "collected for specified, explicit and legitimate purposes" (Article 6.1(b)). Also, personal data must be "adequate, relevant and not excessive in relation to the purposes" of collection (Article 6.1(c))[98] and "accurate and, where necessary, kept up to date" (Article 6.1(d)). Data must be "kept in a form which permits identification of data subjects for no longer than is necessary" (Article 6.1(e)). IoT stakeholders must respect those principles because – in the vision of EU privacy authorities (as gathered in the WP29) - they "play an essential role in the protection of data."[99]

A peculiar concern for IoT data is that the collection can happen "without the individual being actually aware of it;" this should never happen, the WP29 recommends.[100] Also, data should not be "collected and stored just in case or because it might be useful later."[101] IoT stakeholders should also offer users the option of an anonymous service, when that service does not need the collection of personal data.[102] The "data minimization" principle also requires IoT stakeholders to keep the data "for no longer than is necessary for the purpose for which the data were collected or further processed;"[103] in case a stakeholder delivers multiple services and/or the service is delivered by more than one stakeholder, this evaluation must be service specific and stakeholder specific. To be sure, in a subscription service, data should be deleted "as soon as the user puts an end to his subscription" and if users delete information from their accounts, IoT stakeholders cannot retain this information in their files.[104] Further, after a defined period in which a user does not use the service, that user's profile should be changed to "inactive." After an additional period of inactivity, and upon notice to the user, the profile should be deleted.[105]

- *Article 8 (processing of sensitive data).* Importantly, sensitive data is often implicated in the IoT, especially with "Quantified Self" IoT such as sleep trackers and other health-related devices, because these devices mainly register data on individuals' health.[106] Article 8 of the Directive prohibits the processing of "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and … concerning health or sex life" without consent of the data subjects (save other very limited exceptions).[107] Therefore, if the IoT device collects sensitive

---

[97] Opinion on IoT at 16.
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] *Id.* at 16. Internal quotation marks omitted.
[102] *Id.* at 17.
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*
[107] The GDPR deals with the now called "special categories of personal data" in Article 9 and defines this data as personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of genetic data, biometric data in order to uniquely identify a person or data

data, the controllers must obtain the "user's explicit consent, unless the data subject has made himself the data public."[108] The GDPR gives a wider definition of this special category of data (which now includes genetic and biometric data);[109] as a result IoT stakeholders will have to require "explicit consent" in more cases than before.

- *Articles 10 and 11 (transparency requirements).* These principles, which the WP29 finds applicable to IoT processing, basically require data controllers to provide users with a privacy policy in a "clear and comprehensible manner."[110] This might be challenging in the IoT and might require new methods of delivery. The WP29 suggests "this information could be provided for instance on the object itself, using the wireless connectivity to broadcast the information, or using location through privacy preserving proximity testing done by a centralised server to inform users that are located close to the sensor."[111]

- *Article 17 (security requirements).* The WP29 gives a very detailed analysis of IoT stakeholders' duties under Article 17 of Directive 46/1995,[112] and it makes clear that "any stakeholder that qualifies as a data controller remains fully responsible for the security of the data processing" (and this is true also when more than one IoT stakeholder intervenes in the delivery of a specific IoT service). The WP29 discusses new security principles from the GDPR: (i) security breach: the IoT data controller is responsible if the breach results from poor design or maintenance of the device;[113] (ii) security assessments: IoT stakeholders must perform assessments "of system as a whole, including at components' level."[114]

IoT stakeholders that bear responsibility as controllers must supervise those subcontractors that design and manufacture the devices but that are not processors --and therefore not bound by Article 17 – and must seek from them "high security standards with regard to privacy."[115] IoT stakeholders must

---

concerning health or sex life and sexual orientation", which can be processed subject to consent or limited exceptions. Article 9 GDPR.

[108] Opinion on IoT at 17.

[109] *See supra* note 108.

[110] Opinion on IoT at 18. The duty to inform users of the processing is contained in Article 14 and 14(a) of the GDPR (we note that the new right to portability must be specifically listed in the privacy policy). The characteristics of the information are listed in Article 12 of the GDPR. Once the GDPR comes into effect, IoT stakeholders should refer to those provisions for the list of information for users.

[111] *Id.* at 18.

[112] The Article provides for a duty of implementation of "appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing" with "appropriate" to be evaluated "having regard to the state of the art and the cost of their implementation" and the level of risks. Article 17.1.

[113] Opinion on IoT at 18. The GDPR provides for the security of the processing in Article 30 (and introduces a data breach notification duty to the supervisory authority within 72 hours in Article 31).

[114] Opinion on IoT at 18. The WP29 advises IoT stakeholders to apply principles of "composable security," to seek device certification, and to align themselves with "internationally recognized security standards." *Id.* On composable security, *see, e.g.*, Ran Canetti, *Universally Composable Security: A New Paradigm for Cryptographic Protocols*, http://eprint.iacr.org/2000/067.pdf.

[115] Opinion on IoT at 18.

implement security measures "taking into account the specific operational constraints of IoT devices," such as the absence of encryption and the "limited resources in terms of energy and computing power."[116] To respond to these security issues, the WP29 advises the IoT stakeholders to apply the principle of "data minimization" and to restrict the processing of personal data to no more than strictly required.[117] Other recommended practices are "network restrictions, disabling by default noncritical functionalities, preventing use of un-trusted software update sources" and again adherence to a "privacy by design" principle. [118]

The WP29 stresses the importance for cybersecurity in IoT of automatic updates to patch vulnerabilities, which should always be available to users. If this is impossible (for example, because a device is no longer supported by its manufacturer), alternatives should be offered (for example, "opening the software to the open-source community"),[119] and stakeholders should also notify users of the vulnerability.[120]

IoT stakeholders should particularly protect users from hackers' tampering with the security of those IoT devices tracking health values (e.g., sleep trackers) because users can make "health-related decisions" based on those values.[121]

Lastly, data breach notification policies are useful to contain the consequences of vulnerabilities in software and design.[122]

The WP29 also makes clear that in an IoT environment, data subjects maintain the same rights that they currently have (*e.g.*, Articles 12 and 14 of Directive 95/46/EC), particularly the right of access,[123] the right to withdraw consent, and the right to oppose the processing.

In addition, IoT stakeholders must comply with Article 5(3) of Directive 2002/58/EC (consent to storage

---

[116] *Id.* The WP29 notes also that "the common technologies currently in use" are hardly possible in an IoT environment, so IoT stakeholders "need to use secure and lightweight protocols that can be used in low resource environments." *Id.*
[117] *Id.* at 19.
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] This principle is in Article 15 of the GDPR. The WP29 makes clear that access to raw data should be granted to IoT users. Opinion on IoT at 20. The possibility of accessing data is important in case a user want to switch to another provider. *Id.* The WP29 reminds IoT stakeholders that the GDPR provides a "right to portability" and therefore "[d]ata interoperability standards could be usefully developed to that effect." *Id.* The "right to portability … aims at putting a clear end to situations of user 'lock –in'." *Id.* This is another example of the WP29's talking in terms of the new GDPR (and not old Directive). The "right to portability" is in Article 18 of the GDPR:

> The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured and commonly used and machine readable format and have the right to transmit those data to another controller without hindrance from the controller to which the data have been provided.

in E-Privacy Directive).[124] It is not infrequent that an IoT stakeholder wants to gain access to the data stored on the device (such as the WP29's example of a pedometer that registers the steps of the user, who then uploads the data to his computer, with the manufacturer storing the data on its servers). If this is the case, unless the storage or the access is "strictly necessary in order to provide a service explicitly requested by the subscriber or user," then the user or subscriber must provide his or her consent.[125]

To facilitate the application of general EU privacy law to the IoT, the WP29 Opinion includes a list of recommendations, which are divided as follows: (i) all stakeholders; (ii) device manufacturers; (iii) application developers; (iv) social platforms; (v) IoT device owners; and (vi) standardisation bodies and data platforms.[126] The recommendations echo the critical points discussed above as privacy challenges.

D. Mauritius Declaration and other important authorities

Another important document concerning the IoT under an EU perspective is the *Mauritius Declaration on the Internet of Things.*[127] Privacy Commissioners from around the world (*i.e.*, the national authorities with responsibility to supervise and enforce data protection in the several countries) adopted this short and principled Declaration after speakers from the private sector and from academia presented risks and benefits of the IoT. The Commissioners highlight the concern for individuals' right to self-determination, which is an "inalienable right for all human beings" and which can entrench the IoT. [128] The Commissioners' concern is that data from the IoT are "high in quantity, quality and sensitivity" and allow the drawing of broader and more sensitive inferences. The Declaration makes the point that, with the IoT, "identifiability becomes more likely than not."[129] The Commissioners express their opinion that "big data derived from internet of things devices ... should be regarded and treated as personal data."[130] Also, they warn that whatever the business model of the commercial IoT stakeholders might be, the money-making machine is the data.[131] They remind us that

---

[124] *Id.* at 14.

[125] *Id.*

> The consent requirement in Article 5(3) primarily concerns the device manufacturer, but also all stakeholders that want to have access to this aggregated raw data stored in this infrastructure. It also applies to any data controller who wants to store additional data on a user's device. *Id.*

WP29 recalls also to this effect its *Opinion 02/2013 on apps on smart devices* (WP202), http://ec.europa.eu/justice/data-protection/article- 29/documentation/opinion recommendation/files/2013/wp202_en.pdf.

[126] Opinion on IoT, at 21-24.

[127] *Mauritius Declaration on the Internet of Things*, adopted on October 14, 2014 inside the 36th International Conference of Data Protection and Privacy Commissioners ("Mauritius Declaration"), http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf.

[128] "Self determination is an inalienable right for all human beings. Personal development should not be defined by what business and government know about you. The proliferation of the internet of things increases the risk that this will happen." Mauritius Declaration at 1.

[129] Mauritius Declaration at 1. On identifiability, *see, e.g.*, Ronald Leenes, *Do They Know Me? Deconstructing Identifiability*, http://www.uoltj.ca/articles/vol4.1-2/2007.4.1-2.uoltj.Leenes.135-161.pdf.

[130] Mauritius Declaration at 1.

[131] *Id.*

in this society of more and more ubiquitous connectivity, all players have the responsibility (also toward new generations) to maintain trust in a connected world.[132] This trust can be maintained only with "transparency" and to this effect IoT stakeholders currently do not do enough.

The Commissioners indicate concerns and give practical suggestions to the IoT stakeholders and, in doing so, they echo the WP29's concepts of clarity of information, informed consent, privacy by design, and encryption.

First, the Commissioners took issue with lack of clarity. IoT stakeholders today seem more concerned with shielding themselves from litigation[133] than offering clear and understandable information about the data they collect, the purpose of collection and the retention policy,[134] which instead is the key to avoid what the Commissioners call "out-of-context surprises for customers."[135] Today, because the information provided is so poor, user consent is hardly ever informed.[136]

Second, the Commissioners stress the importance of incorporating protective measures (but more generally "data protection and consumer privacy") from the outset of processing, which is the very moment at which collection starts.[137] To this effect, it is important to develop new technologies and new ways of operating, including "[p]rivacy by design and default," which should become the norm in IoT.[138]

Third, the Commissioners emphasize that the IoT poses "significant security challenges" which must be addressed by the IoT stakeholders with something more that "simple firewall."[139] The Declaration favors local processing (*i.e.*, the processing of data on the device itself) over data transmission, and recommends end-to-end encryption when a transmission is necessary.[140]

We mentioned the concept of "privacy by design." In this regard, the eighty-page report of the European Union Agency for Network and Information Security, ENISA -- *Privacy and Data Protection by Design – from policy to engineering December 2014* ("ENISA's Report") – is particularly useful.[141] The Report aims at promoting "the discussion on how privacy by design can be implemented with the help

---

[132] *Id.* at 1-2.
[133] *Id.* at 2.
[134] *Id.*
[135] *Id.*
[136] *Id.*
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] ENISA, *Privacy and Data Protection by Design – from policy to engineering December 2014,* available for download at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design. The ENISA's Report starts with making the point that "Privacy is a fundamental human right. This is acknowledged by Article 8 of the European Convention on Human Rights, which provides a right to respect for one's "private and family life, his home and his correspondence." *Id.*

of engineering methods."[142] ENISA opines that

> privacy needs to be considered from the very beginning of system development. For this reason, [Dr. Ann] Cavoukian [former Information and Privacy Commissioner of Ontario, Canada] coined the term "Privacy by Design", that is, privacy should be taken into account throughout the entire engineering process from the earliest design stages to the operation of the productive system.[143]

ENISA points out that privacy by design is "a multifaceted concept" which is neither "a collection of mere general principles nor can it be reduced to the implementation of [privacy-enhancing technologies] PETs".[144] In fact, it is a process involving various technological and organisational components, which implement privacy and data protection principles. These principles and requirements are often derived from law, even though they are often underspecified in the legal sources.[145] ENISA recognizes the importance of introducing in the general data protection law (the GDPR) the principle of privacy by design, with the correlated concepts of "data protection impact assessment, accountability and privacy seals."[146]

The ENISA's Report clarifies that "[t]he principle 'Privacy/data protection by design' is based on the insight that building in privacy features from the beginning of the design process is preferable over the attempt to adapt a product or service at a later stage."[147]

The Report discusses also the correlated concept of "privacy/data protection by default," meaning that "in the default setting the user is already protected against privacy risks."[148] The Report discusses "privacy design strategies"[149] and several privacy techniques[150] including authentication,[151] attribute based credentials,[152] secure private communications like encryption,[153] and communications anonymity and pseudonymity.[154] The Report offers conclusions and recommendations and can be "a first step towards establishing a set of guidelines for designing privacy-friendly and legally compliant products and services."[155]

---

[142] *Id.* at iii.
[143] *Id.* at 2.
[144] *Id.* at 3.
[145] *Id.*
[146] *Id.* at 3.
[147] *Id.* at 11.
[148] *Id.*
[149] *Id.* at 16-21.
[150] *Id.* at 22-47.
[151] *Id.* at 22.
[152] *Id.* at 24.
[153] *Id.* at 27.
[154] *Id.* at 29.
[155] *Id.* at 47.

Generally speaking, privacy by design and by default should become the cornerstone of the IoT, and stakeholders should carefully study the ENISA's Report.[156] National DPAs also recommend this approach for IoT. For example, the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*), while issuing a resolution starting a public comments period on the IoT, invited the IoT stakeholders to apply privacy by design, as "described in the report published by ENISA." [157]

European national privacy authorities (and other enforcement agencies) are also focusing their attention on the possible risks of the IoT. For example, the mentioned resolution of the Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*),[158] focuses on the same issues of the WP29's Opinion on IoT: the importance of transparency of information, consent, data quality, influence of extensive monitoring on users' behavior, need for security measures, encryption, privacy-by-design, anonymization techniques, portability, fostering of international certification, and others.[159] The results of the consultation have not been published as yet.

The United Kingdom DPA, ICO (Information Commissioner's Office), issued a document discussing, among others, the privacy issues of the IoT. [160] The ICO focuses on consumers' "lack of understanding … as to how and when their data is being collected and the uses to which it may be put … [which are] likely to increase as big data and the Internet of Things tend to use data that is observed, derived and

---

[156] This approach is recommended both by WP29 (Opinion on IoT at 3, 19, 21 and 23) and by the privacy Commissioners gathered in Mauritius (Mauritius Declaration at 2).

[157] Garante per la Protezione dei Dati Personali, *Avvio della Consultazione Pubblica su Internet delle Cose (Internet of Things)* - Deliberazione del 26 marzo 2015, doc. web n. 3898704, available in Italian at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3898704 ("Consultation"). The Italian DPA highlights the following as the points of main concern on which the acquisition of comments and suggestions are appropriate: 1) users' (sometimes unaware users') profiling; 2) need to offer transparent information to users (sometimes necessary to acquire consent): 3) risks connected to the quality of data, to the monitoring or influencing of users, to cybersecurity and security measures; 4) applicability of privacy and data security by design; 5) encryption and data anonymization; 4) business models used;
5) standardization; 6) adoption of certification instruments or authentication to mutual direct or indirect recognition. *Id.*

[158] *See supra* at 158. In Italy also the Telecom Authority (AGCOM) opened for public comments on the M2M as a first step to draft regulations. Delibera n. 708/13/CONS. After studying the results the survey, AGCOM established a permanent working group to study M2M issues. Delibera n. 459/15/CONS, available in Italian at http://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_kidx9GUnIodu&p_p_lifecycle=0&p_p_col_id=column-1&p_p_col_count=1&_101_INSTANCE_kidx9GUnIodu_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_kidx9GUnIodu_assetEntryId=2549747&_101_INSTANCE_kidx9GUnIodu_type=document.

[159] Consultation, *supra* at 158.

[160] ICO, *The Information Commissioner's Office response to the Competition & Markets Authority's call for information on the commercial use of consumer data*, https://ico.org.uk/media/about-the-ico/consultation-responses/2015/1043461/ico-response-to-cma-call-for-evidence-on-consumer-data-20150306.pdf.

> Given the difficulties of 'notice and consent' in a big data / IoT context, certification and assurance are important in ensuring data processing complies with DP requirements. Existing legal mechanisms such as consent and privacy policies are being superseded by technological developments. As data use grows exponentially, it is vital to give consideration to new regulatory solutions, within the existing legislative framework to protect the rights of individuals, in an easy to understand, effective way. *Id.* ¶ D13.3.

inferred, rather than provided deliberately by individuals".[161] Also, the ICO highlights the fact that people are often unaware that their data is collected and analyzed,[162] notes the inadequacy of privacy policies, the obsolescence of consent because of the pace of technological development and the appropriateness of a new regulatory framework. In ICO's view, a possible solution is in privacy seal schemes approved by the DPA. The privacy seals, operated by accredited third parties, "will be awarded to organisations who can demonstrate compliance with the Data Protection Act, good privacy practice and high data protection standards that go beyond the requirements of the Act."[163]

The Spanish DPA, Agencia Española de Protección de Datos (AGPD)[164] discusses the IoT in its strategic plan 2015-2019, approved on November 20, 2015.[165] AGPD highlights how the information available on people has increased in quantity and range and that nowadays it is possible to learn

> practically the totality of the habits and behavior of a person starting from his or her location delivered by his or her mobile, the pictures stored in the cloud or taken by the cameras around the city … On this respect, technological developments like the internet of things or the big data increase and will more and more increase these trends.[166]

Because the IoT will dramatically increase in the next few years and will have an impact on privacy, AEPD resolved to develop projects and analysis about the so-called "connected society," including "big data, internet of things … smart cities, smart cars, [and] smart homes."[167]

The French DPA (Commission Nationale de L'informatique et des Libertés - CNIL) discusses the IoT in its 2014 Annual Report (released in April 2015),[168] mentioning the WP29 Opinion on IoT[169] and the Mauritius Declaration,[170] and placing smart cars[171] and smart cities[172] (specific instances of IoT) among its priorities for the months to come.

---

[161] *Id.* ¶ B7.1.

[162] *Id.* ¶ B8.4.

> The rise of big data and the Internet of Things mean that personal data is often collected and analysed in unexpected ways, for example phone location data and metadata from social media. For instance, do people understand that Twitter data is sold via third parties even if they have read Twitter's privacy policy? *Id.*

[163] *Id.* ¶ D13.4.

[164] http://www.agpd.es/portalwebAGPD/index-ides-idphp.php.

[165] *Resolución de 20 de noviembre de 2015, de la Agencia Española de Protección de Datos, por la que se aprueba el Plan Estratégico 2015-2019*, available in Spanish at http://www.agpd.es/portalwebAGPD/LaAgencia/common/Resolucion_Plan_Estrategico.pdf.

[166] *Id.* at 4-5 (English translation by author).

[167] *Id.* at 39 in Actuación 2.5. Estudios e informes sobre iniciativas y proyectos de carácter tecnológico. English translation by author. *See also* for Spain: *Nuevos Negocios y Aplicaciones: Big Data y la evolución del Internet de las Cosas*, in Spanish at http://www.apep.es/nuevos-negocios-y-aplicaciones-big-data-y-la-evolucion-del-internet-de-las-cosas/.

[168] Commission Nationale de l'Informatique et des Libertés, Rapport d'Activite' 2014, in French at https://www.cnil.fr/sites/default/files/typo/document/CNIL-35e_rapport_annuel_2014.pdf.pdf.

[169] *Id.* at 61.

[170] *Id.* at 65.

[171] *Id.* at 69.

[172] *Id.* at 70.

IV. The U.S. Approach to IoT Law

A. Federal Approach

The US has so far taken a largely self-governing approach to the IoT law. While manufacturers race to create the next connected device, government agencies caution them to be aware of privacy and security concerns. Federal Trade Commission ("FTC") Chairwoman Edith Ramirez cautioned attendees at the 2016 Consumer Electronics Show to be careful about the personal information that is being collected, how it is used and how it is secured, warning that consumers will be hesitant to use these products if they are concerned about privacy and security.[173] Indeed, consumers are concerned about those issues. A 2015 PEW Research Center survey found that a majority of US adults felt they had lost control over how personal information was collected and used by companies, had low levels of trust in government and business sectors who collect and monitor data, and had little confidence in commercial and governmental institutions to maintain the security of their personal information.[174] A 2014 survey found that 87% of consumers were concerned about the type of information collected through smart devices.[175]

1. 2016 FTC Report

In January 2016, in an effort to encourage businesses to enhance and protect consumers' privacy and security, the FTC issued a report ("FTC Report") recommending a series of concrete steps for manufacturers of IoT devices. The FTC Report noted security risks to consumers arising from such devices, including unauthorized access and misuse of personal information, attacks on other systems through these devices, and personal safety risks.[176] In addition, the Report noted privacy risks from the collection of "personal information, habits, locations, and physical conditions over time," information that may be used by companies to make credit, insurance, and employment decisions.[177]

To address these risks, the Report made recommendations in four main areas.

First, it recommended the implementation of security measures for companies developing IoT, including security-by-design (building security into devices at the outset); training employees about

---

[173] Dawn Chmielewski, *FTC Head Calls for Greater Transparency on Data Collected by Internet of Things* (Jan. 6, 2016), http://recode.net/2016/01/06/ftc-head-calls-for-greater-transparency-on-data-collected-by-internet-of-things/?utm_source=linked&utm_medium=social.

[174] Lee Rainie, *Americans Conflicted About Sharing Personal Information with Companies, Pew Research Center* (Dec. 30, 2015), http://www.pewresearch.org/fact-tank/2015/12/30/americans-conflicted-about-sharing-personal-information-with-companies/.

[175] TrustE Privacy Index, 2014 Internet of Things Edition, https://www.truste.com/resources/privacy-research/us-internet-of-things-index-2014/.

[176] Federal Trade Commission Staff Report (2015) ii. *See* FTC Press Release, *FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks* (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

[177] *Id.*

security; and ensuring the security capabilities of outside service providers. The Report also recommended that companies employ multiple layers of security to defend against particular risks; prevent unauthorized access to consumers' devices, data, or personal information; and monitor and provide security patches for connected devices throughout their expected life cycle.

Second, the FTC Report advocated data minimization: companies should limit the data they collect and retain, and dispose of data once no longer needed. This addresses potential harms arising from vast stores of data, like data breaches or use of information for unintended purposes. Third, the FTC recommended that companies notify consumers and give them choices about how their information will be used, particularly when the data collection is beyond their reasonable expectations.

The Report found that specific legislation regarding the IoT would be premature at this point in light of the "great potential for innovation in this area." Instead, the Report encouraged the development of "self-regulatory programs designed for particular industries" to encourage the utilization of privacy- and security-sensitive practices. The Report did call for strong data security and breach notification legislation, and reiterated the FTC's call for broad-based federal privacy legislation. It also noted its continued enforcement of the FTC Act and other laws that apply to the IoT.[178]

Other government agencies agree that the self-governing aspect of the FTC's approach is necessary. In an address to IoT industry leaders, the Federal Bureau of Investigation's Chief Information Security Officer noted that technology companies and organizations are working on developing industry standards and regulations for IoT security: "This is only going to happen through self-regulation because, frankly, you are all moving way too fast for the government to be able to catch up with you," she said. "Self-regulation is critical to this [IoT security] effort."[179]

The self-governing approach to the IoT echoes the federal government's approach to online privacy law in general, as the Report notes in its discussion of the Fair Information Practice Principles.[180] Over a decade ago, the FTC determined to follow the existing self-regulation model because it was "the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology."[181] Proposed substantive legislation regulating websites' treatment of personal information was jettisoned in favor of "best practices guidelines" and "fair information practices" that encourage disclosure and recommend other privacy practices like security measures and consumer options.[182]

---

[178] FTC Report at viii.
[179] Olivia Eckerson, *FBI CISO warns of IoT data breaches* (Sep. 23, 2015), http://internetofthingsagenda.techtarget.com/news/4500254067/FBI-CISO-warns-of-IoT-data-breaches.
[180] FTC Report at 19.
[181] *Self Regulation and Privacy Online*, Before the House Commerce Subcomm. On Telecom., Trade, and Consumer Protection, 106th Cong., Jul. 13, 1999, available at http://www.ftc.gov/os/1999/07/pt071399.htm.
[182] FTC, *Fair Information Practice Principles*, http://www.ftc.gov/reports/privacy3/fairinfo.htm. The four FIPP include Notice & Awareness, Choice & Consent, Access & Participation, and Security & Integrity.

2. Other Applicable Federal Law

While not tailored to the IoT, much existing federal legislation is implicated by it. Title I of the Electronic Communications Privacy Act ("ECPA") is aimed at protecting the privacy of communications by prohibiting the interception of electronic communications in transit.[183] Title II of the ECPA (also known as the "Stored Communications Act"), prevents improper access to "stored" electronic communications and records.[184] The Computer Fraud and Abuse Act is aimed at computer hackers and prohibits unauthorized access to a protected computer.[185]

Other laws follow a sectoral approach of focusing on specific privacy concerns. The Fair Credit Reporting Act regulates the collection, maintenance and dissemination of personal information by "consumer reporting agencies."[186] Additional law protects "customer proprietary network information" from disclosure by telecommunications carriers,[187] regulates how federal governmental agencies gather and handle personal data,[188] and requires financial services companies to implement measures to protect the security and confidentiality of their customers' personal information.[189] The "CANSPAM Act" regulates the treatment of personal information in the form of email addresses by prohibiting the sending of "unsolicited" email and of misleading header information.[190] In addition, legislation restricts the use and disclosure of certain specific types of personal information, including individually identifiable health information,[191] education records,[192] and consumer reports.[193]

More generally, the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce."[194] The FTC has for over ten years now used its enforcement authority under the unfairness prong to bring actions against companies both for privacy misrepresentations and for failure to use "readily available security measures" resulting in a data breach. In *FTC v. Wyndham Worldwide Corp.*,[195] the Third Circuit suggested two primary sources for a company's determination of the reasonableness of its security practices, the FTC's online "checklist" of practices that form a "sound data security plan,"[196] and previous FTC complaints and consent decrees in administrative cases raising

---

[183] 18 U.S.C.A. § 2710 *et seq.*
[184] 18 U.S.C.A. § 2701 et seq.
[185] 18 U.S.C.A. § 1030(a)(2)(C).
[186] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*
[187] 47 U.S.C. § 222.
[188] Privacy Act of 1974, 5 U.S.C. § 552a.
[189] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*
[190] Controlling the Assault of Non-Solicited Pornography & Marketing Act of 2003 (CANSPAM Act), 15 U.S.C.A. § 7701 *et seq.*
[191] Health Insurance Portability and Accountability Act (HIPPA), 29 U.S.C. § 1181.
[192] Family Education Rights and Privacy Act, 20 U.S.C. § 1232.
[193] 15 U.S.C. § 1681 *et seq.*
[194] 15 U.S.C. § 45(a)(1)-(2) (2000).
[195] 799 F.3d 236 (3d Cir. 2015).
[196] *Wyndham* at 257, *citing* FTC, *Protecting Personal Information, A Guide For Business* (Nov. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

unfairness claims based on inadequate corporate cybersecurity.[197]

The FTC brought its first case involving an Internet-connected device in 2013 against TRENDnet.[198] The company's Internet-connected security cameras were equipped with faulty software, making them vulnerable to hackers who were able to access live feeds from customers' security cameras and view sleeping infants and other private home activities. The FTC's settlement with TRENDnet prohibited it from misrepresenting the security of its cameras or the extent to which a consumer can control the security of information the cameras transmit, and required the company to establish a comprehensive information security program, obtain regular security assessments, and notify customers about the cameras' security issues and the availability of corrective software.[199]

B. State Law

States have stepped in to provide legislation in many aspects where federal law has not.[200] A California law that went into effect at the beginning of 2016 targets smart televisions that have voice recognition features, and requires manufacturers of those TVs to prominently inform users of those features during the initial setup or installation.[201] The bill also restricts manufacturers and third parties who contract with them from selling or using for any advertising purpose any actual recordings of conversations collected through the voice recognition feature. In addition, the bill prohibits anyone from forcing an entity providing the voice recognition feature to create technology that would allow an investigative or law enforcement officer to monitor communications through that feature. California also has criminal laws that are implicated by the IoT, one that prohibits television corporations from using any electronic device to record or eavesdrop on subscribers without their consent,[202] and one that makes it a misdemeanor to publish identifiable nude pictures online without the subject's permission.[203]

California and Delaware have laws relating to children's online privacy, including limitations on marketing and advertising and certain uses of personally identifiable information.[204] California,

---

[197] *Wyndham* at 257.
[198] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.
[199] FTC Press Release, *Marketer of Internet-Connected Home Security Video Camera Settles FTC Charges It Failed to Protect Consumers' Privacy* (Sep. 4, 2013), https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.
[200] *See* Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, The New York Times (Oct. 30, 2013), http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html?_r=1.
[201] CA Assembly Bill 1116, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160AB1116.
[202] CA Penal Code Section 637.5, http://law.onecle.com/california/penal/637.5.html.
[203] CA Senate Bill 255, http://www.leginfo.ca.gov/pub/13-14/bill/sen/sb_0251-0300/sb_255_bill_20130821_amended_asm_v95.pdf.
[204] National Conference on State Legislatures, *State Laws Related to Internet Privacy* (Jan. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx.

Connecticut, and Delaware have laws requiring that websites or online services (including mobile applications) include disclosures about the personal information they collect, what they do with it, and with whom they share it.[205] Nebraska and Pennsylvania prohibit false and misleading statements in privacy policies.[206] Eight states have passed laws limiting the use of drones.[207] And all but three states (Alabama, New Mexico and South Dakota) have data breach notification statutes requiring that consumers be notified within a specific amount of time when there is a data security breach.[208]

Finally, every state has a consumer protection statute with general "unfair practices" language similar to federal law. Like the FTC, states use those statutes to police privacy and security practices they deem to harm consumers.

V. Conclusion

In the EU, the trend is to apply the whole of the general data protection law to the IoT. This makes sense in the current legal framework, because the IoT performs operations on personal data (both of users and of unaware bystanders) and this is "processing" under the Data Protection Directive and under the GDPR. However, some of the data protection concepts are hardly appropriate for the IoT. For example, trying to elaborate and mandate the concept of "informed consent" to data processing in a hyperconnected world might be a band-aid solution. When everyone is connected 24/7 to others and/or to things (a kind of the "hive mind" or "collective" consciousness of the Borg in Star Trek), does the concept of "consent" become meaningless? But, already today, if the data are not conferred by users and are instead subject to ubiquitous capture by sensors, and if users must renounce certain key features of a service to preserve their privacy, is the denial of consent a real alternative?

If the framework changes from informed consent, what will be the basis for the protection of privacy? We have some hints of emerging alternatives. *First*, privacy by default and design, which means that privacy features (including encryption) are embedded in the machines from the "outset". *Second*, data minimization and local processing, which means only collecting and transmitting data when strictly necessary. *Third*, multilevel cybersecurity, meaning that IoT stakeholders participating in the process should coordinate to secure the entire IoT "ecosystem," not only their segment. *Fourth*, "privacy seals" to foster enhanced trust of users and nonusers. (Government could provide incentives for many of these alternatives through tax credits.) For these reasons and for other privacy challenges discussed above, the EU should consider specific legislation governing the IoT because the phenomenon has unprecedented features.

In general, U.S. law approaches the IoT with the perspective that, in the fast-moving Internet realm,

---

[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] National Conference of State Legislatures, *Security Breach Notification Laws* (Jan. 4, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

specific legislation is liable to stymie innovation and insufficiently keep up with changing technology. Instead, the government embraces a self-governing model that encourages privacy and security best practices. Because it is in the interest of IoT device manufacturers for consumers to trust these devices, the government hopes its recommendations will be well-received. In the likely event of a privacy or security incident involving the IoT, the FTC will probably step in and bring an enforcement action just as it does in other types of privacy or data breach cases. With the exception of states like California, which has passed far-reaching privacy protections, most states will also fall back on general consumer protection statutes to prosecute abuses by the IoT industry.

Despite the challenges, in both the EU and the US, IoT stakeholders should see privacy and data protection as an opportunity, not as a burden to doing business.

Francesca Giannoni-Crystal *(NY, DC, Italy + SC Foreign Legal Consultant, not a member of SC Bar) is a dually-qualified U.S. and Italian attorney. She holds JDs from Italy (110/110) and the US (cum laude). In her twenty years of practice in Italy and the US she has provided assistance (including in M&A) to a wide range of clients (industrial, commercial, technological, financial, and legal) both domestically and internationally. She worked for Deloitte Legal and in-house for an international group in the internet and mobile sector. She is also a "lawyer for lawyers", assisting law firms in bridging activities (Civil Law-Common law), supporting other lawyers in international litigation (e.g. issues of international privilege and cross border ethics), and aiding in international transactions (e.g. transactional structures, privacy, and foreign corporate issues).*

Ms. Giannoni-Crystal has written and spoken both domestically and internationally on a number of topics in the fields of contract law, professional responsibility, technology and privacy, and comparative law. She is co-responsible for the website www.technethics.com, a database, blogging, and training platform in the fields of ethics & technology and privacy. Ms. Giannoni-Crystal is a member of Crystal & Giannoni-Crystal, LLC, (www.cgcfirm.com) with offices in New York, DC and Charleston, SC. fgiannoni-crystal@cgcfirm.com.

Allyson Haynes Stuart*, Of Counsel with Crystal & Giannoni-Crystal, LLC, is a scholar and practicing attorney focusing on privacy, data security, and e-discovery issues. She is a frequent speaker and writer on those topics and blogs for technethics.com. Professor Stuart has taught law for eleven years, including teaching E-Discovery, Information Privacy Law, Internet Law, Contracts, Civil Procedure and Evidence at the Charleston School of Law. She taught Internet Law as an adjunct at Brooklyn Law School; taught Comparative Privacy Law (the EU and the US) as an adjunct at the Instituto de Empresa in Madrid, Spain, and Stetson University in Granada, Spain; and taught Comparative Intellectual Property (the EU and the US) at Suffolk University in Madrid, Spain. Professor Stuart practiced as a litigator in New York at Cleary, Gottlieb, Steen & Hamilton in New York and served as in-house counsel at Sony Corporation of America before returning to Charleston, SC.*

Making Lemonade out of Lemons: The Cybersecurity Information Sharing Act of 2015

By Jason Edgecombe and Frederick Scholl


On December 18, 2015, President Obama signed the omnibus spending bill for the coming year. Inserted into the final bill was the Cybersecurity Information Sharing Act ("CISA") which, when fully implemented, is intended to create a process to allow the private sector and the federal government to share information concerning cybersecurity threats, distribute that information, and—ideally—inhibit the spread of such threats.

That is the vision, at any rate. But questions still remain, as it is unclear how the information-sharing framework will operate in practice, how it will be implemented, and what threats it will be able to combat. Additionally, from an operational standpoint, CISA has been a lightning rod for privacy advocates and watchdogs, who are concerned that in facilitating data sharing—especially with the government—CISA as-passed does not do enough to protect privacy and civil liberties.

To consider these questions, and hopefully move toward answers, this article will begin with a review of the cybersecurity landscape into which Congress has loosed CISA. We will then review where the best use of the government's resources lie in information sharing and facilitating cybersecurity. Turning to a policy and legal standpoint, we will take special consideration to the privacy aspects of the law; CISA sets a low bar for the protection and non-disclosure of personally identifiable information, and the private sector may determine that business considerations require above-baseline privacy protections; the practical operation of CISA's liability shield; and what factors non-federal entities should consider when making a decision to participate in the information-sharing program.

The Cybersecurity Landscape

CISA did not break new ground in legislating sharing of “cyber threat indicators." Looking at “Google Trends,” we see that the slightly broader term “threat intelligence” appeared in 2011 at a level of interest = 1. It is now at an all-time high of 100 and sharply increasing.[1] Interest in cyber threats, of course, did not appear in a vacuum: in April 2010, Chelsea Manning began leaking significant numbers of classified government documents via WikiLeaks.[2] 2011 was also the year of the Sony PlayStation breach,[3] a Citibank breach of 210,000 card holders’ information,[4] and a Pentagon breach of sensitive defense information,[5] among others. Congress’s response was the 2011 The Cyber Intelligence Sharing

[1] https://www.google.com/trends/explore#q=threat%20intelligence
[2] *See* Associated Press, *Judge accepts Manning's guilty pleas in WikiLeaks case*, Feb. 28, 2013.
[3] *See* Liana B. Baker, *Sony PlayStation suffers massive data breach*, REUTERS, Apr. 26, 2011.
[4] *See* Kim Zetter, *Citi Credit Card Hack Bigger Than Originally Disclosed*, WIRED, June 16, 2011.
[5] *See* Jason Ukman & Ellen Nakashima, *24,000 Pentagon files stolen in major cyber breach, official says*, WASH. POST, Jul. 14, 2011.

and Protection Act ("CISPA"), which quickly engendered a substantial backlash due to a perceived lack of civil liberties and confidentiality safeguards.[6] Under the threat of a presidential veto, CISPA died in the Senate in 2013.[7]

In the meantime, private industry from 2011 to the present has been active in developing better means of cyber information sharing. Participants include vendors of security products and services, industry consortia, as well as end users of security products and services. The value of threat information is well established within information security practice. The basic risk equation illustrates this: risk = threat x asset value x vulnerability. Unless threats are characterized and understood, security risks will not be understood. The challenge is that threats are industry and even organization specific. Unless there is a corresponding vulnerability and asset, there is no threat for that organization. Significant investments are still being made by private industry to improve threat information gathering and sharing. Vendors include specialized firms such as Recorded Future, Cyveillance and iSight Partners as well as enterprise firms such as Cisco, IBM and Symantec. Open source threat intelligence feeds include: OTX, Facebook ThreatExchange, VirusTotal, SpamHaus, and many others. Some industry verticals have taken the initiative to share threat information within their communities. Sharing communities include FS-ISAC (Financial Services), REN-ISAC (Education and Research) and HITRUST (healthcare). State and local government have set up Fusion Centers, to share terrorist threat information. Individual “end user” firms like Citigroup have set up internal fusion centers for cyber information sharing. Finally, professional groups like ISSA have long had groups for Chief Information Security Officers, where threat information is exchanged, along with other best practices.

Thus, it is into this context that Congress passed CISA 2015. In the next section we look at the contents of the Act.

Overview of CISA's Provisions

To begin at the beginning, CISA's sharing framework applies to "cyber threat indicators" and "defensive measures."[8] "Cyber threat indicators" consist of information that is necessary to define or describe "malicious reconnaissance . . . transmitted for the purpose of gathering technical information," "method[s] of defeating a security control or exploit[ing] a security vulnerability," or the existence of a security vulnerability itself.[9] "Defensive measures" are, essentially, any actions, procedures, or other measures that will detect, prevent, or mitigate a cybersecurity threat.[10]

---

[6] *See* Gerry Smith, *Senate Won't Vote On CISPA, Deals Blow To Controversial Cyber Bill*, HUFFINGTON POST, Apr. 25, 2013.
[7] *Id.*
[8] Cybersecurity Act of 2015, H.R. 2029, 114th Cong. § 102(6), (7) (2015) (hereinafter, "CISA").
[9] *Id.* § 102(6).
[10] *Id.* § 102(7). Note, however, that any measure that destroys data or provides unauthorized access to another information system does not meet the definition of a "defensive measure." In other words, you cannot prevent hacking by becoming a hacker yourself. This provision forecloses one of the more salient concerns from CISPA, i.e., that it would let entities "hack back" against perceived threats. *See* D.J. Pangburn, *CISPA's Immunity Provision Would Allow Corporate Hacking*, MOTHERBOARD, Apr. 23, 2013.

Section 103 outlines how the Federal government will share cyber threat indicators with non-Federal entities. This information sharing is to be carried out through existing processes, roles, and responsibilities.

Section 104 contains the legal underpinnings of CISA's sharing provisions, providing that any "non-Federal entity" (that is, private business) may share with or receive from any other non-Federal entity or the federal government a cyber threat indicator or defensive measure, so long as the sharing is "for a cybersecurity purpose."[11]

Section 105 sets forth the mandate to the Department of Homeland Security ("DHS") to develop administrative procedures for the sharing of information with the federal government, including the development of the capability to "accept from any non-Federal entity in real time cyber threat indicators and defensive measures."[12]

Considerations for Implementation

This discussion considers architectural and technical issues that are relevant to the implementation of CISA §103 and §105. Our analysis is based upon "lean thinking," a methodology that focuses on a systems approach emphasizing the end-value delivered and cost of delivery.[13] Under lean, the goal of CISA is not simply information sharing—that is, the process—but on improving cybersecurity in private industry and federal government. What implementation strategy will help meet this objective?

We start by looking at the system private industry-Federal government and then pertinent details of how the information will be shared within CISA.

Role of Government in Cybersecurity Information Sharing

Implementation of CISA ideally would be carried out with a framework for collaboration in cyberspace between government and private industry. But to date, there is no public-private cyberspace governance model from which to draw; there is only a series of one-off actions, taken in response to emergencies. The "Cybersecurity National Action Plan" will address this question in the future,[14] but as of today, any model starts from scratch.

Thus, with no established framework, one possible model for public-private collaboration that warrants attention is Michael Porter's "Shared Value" concept.[15] Porter defines shared value as "policies and operating practices that enhance the competitiveness of [an entity] while simultaneously advancing the economic and social conditions in the communities in which it operates."[16] Applied to

[11] CISA § 104(c)(1).
[12] CISA § 105(a)(3), (c)
[13] *See generally* JAMES P. WOMACK AND DANIEL T. JONES, LEAN THINKING (1996).
[14] "Cybersecurity National Action Plan", February 9, 2016
[15] Michael E. Porter & Mark R. Kramer, *Creating Shared Value*, HARVARD BUS. REV. (Jan.–Feb. 2011).
[16] *Id.*

cybersecurity, the community is clearly the Internet. Literally, everyone is connected via the Internet. Porter goes on to apply his concept to government and partnerships with private industry. His conclusion in this arena is: "benefits are delivered by those organizations that are best positioned to achieve the most impact for the least cost." CISA is a public-private partnership. The "shared value" concept can help in getting the most value out of this partnership.

Looking at implementation details from a shared value perspective, CISA information sharing could be configured in several ways. First, government could be an active participant, inserting itself into the threat mitigation actions of private industry. Government would then be a partner in real time, sharing threat indictors. Second, government could also act as a facilitator, helping create an environment in which private industry can succeed in sharing threat intelligence within its own communities. A third option would be to use some combination of the first two approaches. We have already seen that, since 2011, private business has made significant progress with threat intelligence sharing.[17] Given that the government is entering a relatively developed field, should government facilitate these existing activities or add new communication channels?

In arriving at an answer, it is important to distinguish the different types of threat intelligence. The three classifications are: tactical intelligence, operational intelligence, and strategic intelligence. Tactical information includes IP addresses, URLs and other raw information that may indicate an attack. Operational intelligence adds TTPs, the techniques, tactics and procedures used by cybercriminals. Finally, strategic information includes insight into security trends, allowing organizations to invest in next years' attacks, not only this years'. Tactical information and operational information must be shared in real time, or near real time; strategic information may be shared with monthly or quarterly updates.

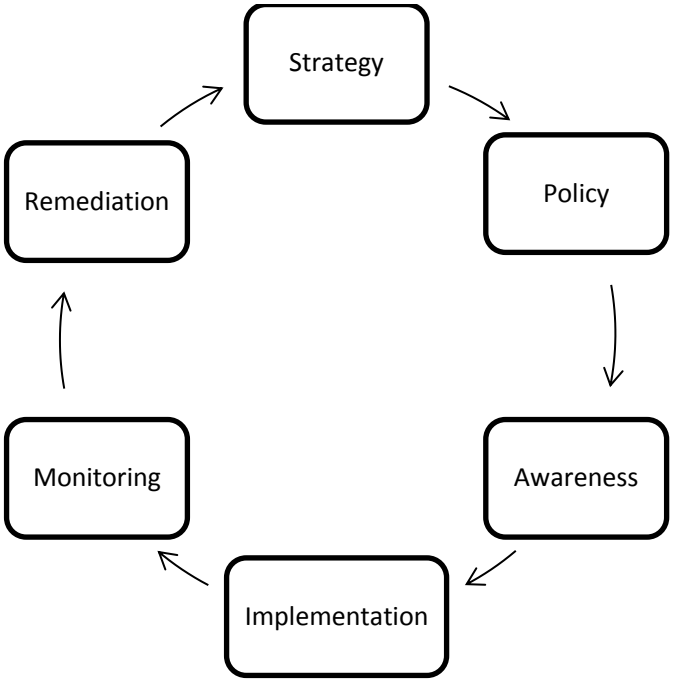
Under CISA's framework, the government's principal role is to facilitate tactical and operational intelligence, that is, pushing out the day-to-day intelligence that is generated concerning cybersecurity threats. Indeed, CISA explicitly contemplates this role in directing DHS to create a "real time" process for disseminating threat indicators between the government and the private sector.[18] Congress did contemplate that the Federal government would also share cybersecurity best practices with non-Federal entities. This is already happening; under CISA more such sharing may take place.

Security Must Be Holistic

Security is only effective in the long term when it is a continuous process, designed as a system. Improving one area of security without considering downstream effects often will not result in any improvement in security. Whether private industry/federal government collaboration is carried out at the tactical, operational, or strategic level, this principle must be followed.

---

[17] *See supra* n. 3 & accompanying text.
[18] *See* CISA § 105(c)(1).



Phases of information security lifecycle

One way of illustrating this process is shown in the Figure, which illustrates the phases of the information security lifecycle.[19] Clearly, this process is holistic; if any step in this diagram is omitted, the effect on the overall security of the organization will be adversely affected. Conversely, addition of new measures—such as the contemplated public-private information sharing—have value only if they can lead to faster, more efficient, or lower cost execution of this security lifecycle. Moreover, the security lifecycle is subject to the overall security budget of the organization; many chief information security officers ("CISOs") still consider lack of budget to be their number one security risk.[20] Building up one phase in isolation does not improve the security process.

If we consider the "Strategy" phase of the lifecycle, today, only the largest firms have access to strategic threat intelligence information, which is generally unavailable to mid-sized and small businesses. Thus, if the government provided more strategic threat intelligence, these firms would benefit.

On the other hand, consider the "Implementation" phase, which is the nuts-and-bolts phase where firewalls are deployed, systems patched, etc. Threat intelligence at this level includes malware signatures, URL reputations, and vulnerability data—that is, tactical intelligence. Currently, there are multiple sources of vulnerability information. Adding more such tactical shared information may

[19] J.L. Bayuk, STEPPING THROUGH THE INFOSEC PROGRAM (2007).
[20] MICHAEL S. OBERLAENDER, C(I)SO—AND NOW WHAT? (2013).

further overload infrastructure managers and decrease security. Moreover, tactical information deals with specific vulnerabilities and therefore is highly organization specific.

Given the amount and specificity of tactical information, it is critical that CISA not to add more *redundant* information. CISA legislates sharing *to* the Federal government and sharing *from* the Federal government. We already have duplicated information flowing from the Federal government; for example, US-CERT sends out the same patch announcements as Microsoft and other vendors.[21] So does MS-ISAC (multi state ISAC) and the FBI. At this point quality of information is more important than quantity, and therefore DHS should develop CISA procedures should reduce redundancies.

Finally, at the operational level, we are dealing with security breach events and incident response (Monitoring phase). This level includes the work of analysts in Security Operations Centers (SOCs), looking for current hacker TTPs. The same information overload is present here. IBM estimates that their clients see an average of 91,000,000+ security events per year and 109 actual security incidents.[22] So more unfiltered information ("false positives") will not improve security, given a fixed overall budget for analysts. Again, DHS should be cognizant of these issues when designing final CISA procedures.

Security Information Must Be Shared Quickly

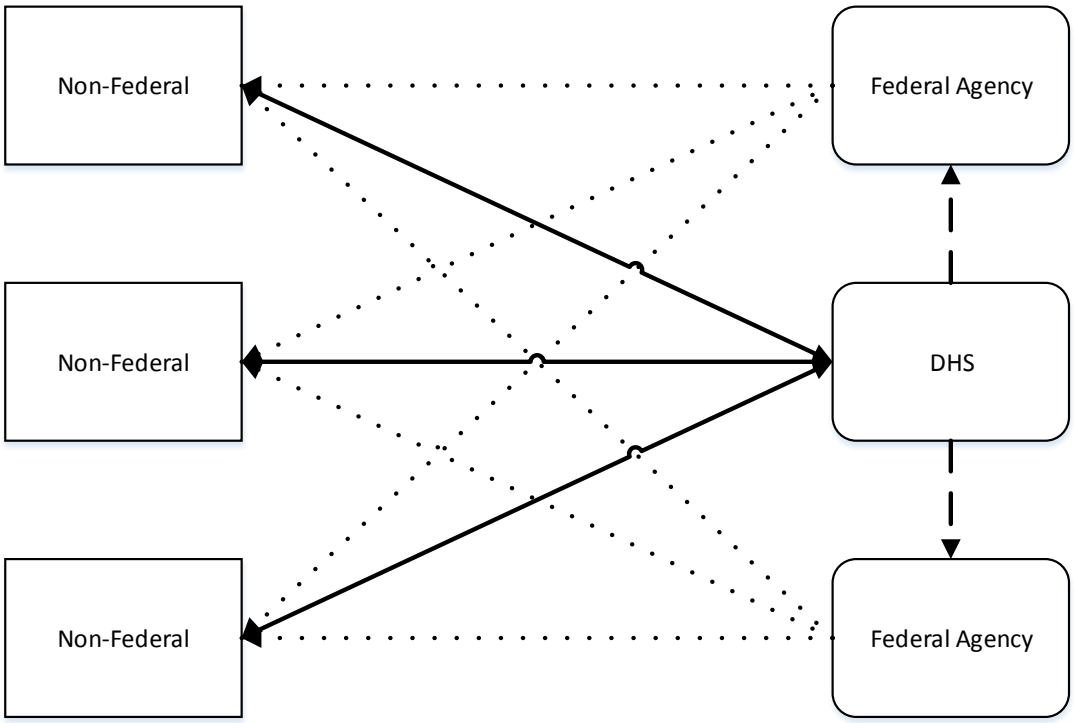
The words "timely" and "real time" appear several times in CISA, so it is clear that Congress is concerned with the speed of the overall process of sharing threat intelligence.

But how fast is fast enough? We already noted that sharing of strategic information such as "cybersecurity best practices"[23] by the Federal government could be done on a quarterly or annual schedule. But how about tactical or operational information? The 2015 Verizon Data Breach Investigations Report provides insight here.[24] The report estimates that 75% of attacks spread from victim #1 to victim #2 in less than 24 hours.[25] Therefore, tactical threat intelligence must propagate from the first victim to all potential victims in less than one day. Furthermore, Verizon's research shows that these threat indicators remain valid for only a few days. After that time, attackers have moved on to new IP addresses, URLs, etc. Threat indicators acted on after this time will simply result in false positives.

Unfortunately, the technical architecture described in CISA has the potential for longer delays.

---

[21] *Compare* https://www.us-cert.gov/ncas/current-activity
[22] IBM Security Services 2014 Cyber Security Intelligence Index
[23] *See* CISA § 103(a)(5).
[24] VERIZON, 2015 DATA BREACH INVESTIGATIONS REPORT (2015).
[25] *Id.* at 10–11.



Information flows specified by CISA

As shown in the Figure, information flows from private industry to DHS, through automated systems to other Federal agencies and then back to private industry, and the Federal government may originate threat indicators as well. Sharing from DHS to other Federal agencies is specified to be real time and automated, but, under CISA, delays can be tolerated if all appropriate Agencies agree. To make this system work for tactical and operational threat information total delays should be less than 24 hours.

CISA's Privacy Framework

Having considered CISA's theoretical and technical framework, let us switch gears and consider the legal framework that surrounds the actual information that the system will be sharing, the effects on privacy, and the implications for non-governmental entities participating in CISA. Prior to enactment, CISA was routinely criticized by privacy watchdogs,[26] who, like Sen. Ron Wyden (D-OR), have called CISA "a surveillance bill by another name."[27]

In order to understand the privacy implications that CISA raises, it is useful to move through the statutory scheme in order to understand where personally identifiable information might get swept up into the system, where it goes, how it may be used, and who is responsible.

[26] *E.g.*, Mark Jaycox, *EFF Opposes Cybersecurity Bill Added to Congressional End of Year Budget Package*, ELECTRONIC FRONTIER FOUND., Dec. 18, 2015.
[27] 161 CONG. REC. S4009 (daily ed. June 10, 2015) (statement of Sen. Ron Wyden).

Initial Collection

To be sure, CISA's statutory language does purport to protect individual user privacy. Section 104 provides:

Removal of certain personal information—A non-Federal entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) Review such cyberthreat indicator to assess whether such cyber threat indicator contains any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

(B) Implement and utilize a technical capability to remove any information not directly related to a cybersecurity threat that the non-Federal entity knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.[28]

Thus, on its face, CISA requires the identification and removal of personally identifiable information; the burdens that it places on non-governmental entities, however, is extremely low. CISA only requires that they remove information that they "*know[] at the time of sharing* to be personal information of a specific individual," and only if such information is "*not directly related* to a cybersecurity threat."[29]

This requirement presents a low bar, and is problematic for several reasons. First, it requires only the removal of personally identifiable information of which the entity has actual knowledge. While the non-governmental entity is directed to "review" the data for personal information, that information would only be subject to removal if it is so obviously personal information such that the sharing party "know[s]" about it without performing perform any sort of pre-sharing diligence. Furthermore, this language leaves open the possibility that the shared data contains combinations of information that, in sum, could "identif[y] a specific individual" in a way that is not obvious upon initial review. The knowledge requirement is also temporally bound to "the time of sharing"; in other words, if the non-governmental entity determines at some later time that personally identifiable information was shared with the government—and then with entities outside the government—there is no requirement to notify the government, to attempt to replace the data with deidentified data, or to take any steps to mitigate the error. Indeed, this limited obligation appears to be the result of a specific decision by Congress, as the version of CISA that originally went through the House required the removal of information "reasonably believe[d]" to be personally identifiable,[30] which would have required a level

[28] Cybersecurity Act of 2015, H.R. 2029, 114th Cong. § 104(d)(2) (2015).
[29] Id. § 104(d)(2)(A) (emphasis added). Note that the same also applies to defensive measures. *Id.* Nevertheless, because of the low probability that defensive measures would include personal information, and for ease of reading, this section generally will refer only to cyber threat indicators.
[30] Protecting Cyber Networks Act, H.R. 1560, 114th Cong. § 104(d)(2) (2015).

of proactive decision making on non-governmental entities before sharing information that is not required in CISA as-enacted.

Second, even if the non-governmental entity knows that it is sharing personally identifiable information, it still would not need to remove such information if it is "directly related to a cybersecurity threat."[31] Might this exception swallow the rule? For example, in a distributed denial of service attack, non-governmental entities might provide to DHS or other private entities with the IP addresses believed to have launched the attack.[32] This sort of information sharing was explicitly contemplated by Congress[33] and permissible under CISA.[34]

If the attack target wanted to share information about the attackers, the most likely way to do so would be to share the all IP addresses of all computers pinging the target during the time of the attack. However, it is likely that any coordinated attack would occur alongside unrelated traffic from innocent users who just happened to be connected to the attack's target at the same time as the attack, and because there is no way to separate the innocent traffic from the attack, the target would need to share it all. Thus, privacy of such innocent users would be compromised at two separate stages. First, it is questionable under U.S. law whether IP addresses even constitute personally identifiable information; some courts have taken the position that an IP address only identifies a computer and not a person, and therefore they are not "personally" identifiable information.[35] Second, because IP addresses are the central indicator for a denial of service attack, IP addresses would be "directly related to a cybersecurity threat," and therefore would be shared under CISA.

In this scenario, innocent users would find their IP addresses swept up in the CISA data collected and then shared with DHS, and then shared with other non-governmental entities through the envisioned system of threat information dissemination. Moreover, this example is simply the most obvious example where user data would be transmitted through CISA. If CISA leaves a privacy gap for common threats, information sharing on other, more sophisticated attacks is likely to have similar results.[36]

---

[31] Cybersecurity Act of 2015, H.R. 2029, 114th Cong. § 104(d)(2) (2015).

[32] ANDREW NOLAN, CONG. RESEARCH SERV., R43941, CYBERSECURITY AND INFORMATION SHARING: LEGAL CHALLENGES AND SOLUTIONS 5 (2015).

[33] *Id.*

[34] CISA § 104(c)(1).

[35] See Johnson v. Microsoft Corp., No. C06-0900RAJ, 2009 WL 1794400, at *4 (W.D. Wash. June 23, 2009); Columbia Pictures Indus. v. Bunnell, 2007 WL 2080419 *3 n.10 (C.D. Cal. May 29, 2007). Notably, these cases addressed only whether IP addresses were "personal information" as contemplated in the specific language of specific contractual user licenses. CISA seems to contemplate explicitly the distinction between information that identifies a computer and that identifies a person when it limits deidentification only to "personal information *of a specific individual* or information that *identifies a specific individual*." CISA § 104(d)(2)(A) (emphasis added). The European Union, by contrast, has determined that users can be identified through IP addresses, and therefore IP addresses are "personal data." See Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 16, 01248/07/EN/WP 136 (June 20, 2007).

[36] Indeed, CISA essentially acknowledges that personal information will be shared when it directs the Department of Justice and DHS to develop procedures for handling personal information. See CISA § 105(b)(3)(B).

DOJ and DHS Guidance

As the example above shows, it is very likely that the sharing of threat indicators through CISA will lead to the sharing of personal information, whether as the result of the nature of the threat itself or the inability to identify personal information before sharing.

CISA directs the Attorney General and Secretary of Homeland Security to jointly develop and issue "guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with [CISA]."[37] The final version of these guidelines is scheduled for publication in summer 2016.[38] In a broad outline of the guidelines, Congress has directed that they should, among other things:

- "limit the effect on privacy and civil liberties of activities by the Federal Government";
- limit the receipt, use, retention, and dissemination of any threat indicators that contain personally identifiable information, including data destruction and retention policies; and
- protect threat indicators containing personal information "to the greatest extent practicable" and create sanctions for unauthorized use of personal information.[39]

On February 16, 2016, DOJ and DHS published their interim privacy and civil liberties guidelines (the "Interim Guidelines").[40] The Interim Guidelines direct federal entities to share information consistently with the White House's 2011 Fair Information Practice Principles of (a) transparency; (b) individual participation; (c) purpose specification; (d) data minimization; (e) use limitation; (f) data quality; (g) security; and (h) accountability and auditing.[41] The Interim Guidelines provide further direction on timely information destruction, controls for safeguarding information, and removal of received information that is not "directly related" to a cyber threat.[42]

For privacy advocates, then, the Interim Guidelines are a step in the right direction. There are, however, several caveats. First, as "guidelines," it is not clear what legal force they will have, how they could be enforced, or who would have legal standing to challenge them. Indeed, the only apparent enforcement mechanism is sanctions on individuals who fail to follow the guidelines.[43] While such sanctions (up to and including termination) can be severe, it is difficult to see how they would police

---

[37] CISA § 105(b)(2)(A).
[38] Id.
[39] Id. § 105(b)(3)(A), (b)(3)(B), (b)(3)(C), (b)(3)(F).
[40] DEPT. HOMELAND SECURITY & DEPT. OF JUSTICE, PRIVACY AND CIVIL LIBERTIES INTERIM GUIDELINES: CYBERSECURITY INFORMATION SHARING ACT OF 2015 (2016).
[41] WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE: ENHANCING ONLINE CHOICE, EFFICIENCY, SECURITY, AND PRIVACY, at Appx. A (2011).
[42] INTERIM GUIDELINES, *supra* note 40, at 7, 10, 11.
[43] *Id.* at 12.

systemic non-compliance within a department or agency.[44] Second, CISA authorizes DOJ and DHS to "periodically, but not less frequently than once every 2 years" review the guidelines and presumably revise them, which could make privacy protections subject to the political priorities of the existing presidential administration.

Third, the Interim Guidelines establish notice procedures for notifying "any United States person whose personal information [is] shared in violation of CISA."[45] However, as we have already discussed, personal information that is shared under the rationale that it is "directly related" to a cybersecurity threat *is not* shared *in violation* of CISA, which likely makes any right to notification essentially hollow.

Fourth, and potentially the most problematic, is that anything in the final guidelines (and any successive revision thereto) must be "consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats."[46] In other words, any privacy or civil liberties concerns expressed in the guidelines are intentionally given a back seat to the need to "protect information systems." How the final guidelines will balance these directives—if they can be balanced—remains to be seen.

Liability

For CISA's proponents, the liability provisions were a key rationale for the law, as they contend that private entities were fearful of alerting the government and one another of cyber threats for legal and liability concerns.[47] Some CISA critics, however, contend that such information sharing is already occurring absent CISA's permissions or protections,[48] and, as discussed above, private industry has spent the past five years filling the void of government inaction.

Section 106 provides that "[n]o cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing of" threat indicators or defensive measures pursuant to CISA.[49] Note that Section 106 grants an immunity to liability, offering what amounts to an affirmative defense and the basis for any court to grant a motion to dismiss at the pleadings stage.[50]

While the grant appears broad, it is worth considering how it interacts with other CISA provisions, as doing so uncovers certain pitfalls for the unwary.

---

[44] *Id.*
[45] *Id.* at 9.
[46] Id. § 105(b)(3).
[47] See Erik Barnett, *Bridging the Intelligence Gap: Cybersecurity Information Sharing Act of 2015*, http://blog.algosec.com/2015/11/bridging-the-intelligence-gap-cybersecurity-information-sharing-act-2015.html (last visited Feb. 10, 2016) (reporting on a panel of banking security executives who stated that "[t]here were policies and laws that basically prevented them from cross sharing cyber attack information.").
[48] *See* Robert Graham , *Whatever it is, CISA isn't cybersecurity*, http://blog.erratasec.com/2015/03/what-ever-it-is-cisa-isnt-cybersecurity.html (last visited Feb. 10, 2016).
[49] *Id.* § 106(b).
[50] *See id.* (any lawsuit "shall be promptly dismissed").

With respect to sharing with the government, a private entity must ensure that the sharing take place "in a manner that is consistent with"[51] the process that DHS develops to receive and disseminate threat indicators and defensive measures in order to qualify for the immunity.[52] As set forth in the Interim Guidelines, this means using DHS's Automated Indicator Sharing ("AIS") capability,[53] which provides for intake via web portal, email, or an automated Structured Threat Information eXchange ("STIX").[54] Given that a private entity need not follow the DHS procedures to the letter but only share data "in a manner that is consistent with" them, this provision amounts to a striking grant of immunity to any private entity that gets the process mostly correct.

That requirement, however, only applies to information that is shared through the federal government. CISA, however, also provides the ability for private entities to share information directly with one another,[55] and an entity undertaking such sharing would not need to conform to DHS procedures in order to receive the immunity.

Nevertheless, private entities still must be careful in that they will *not* receive the immunity unless the sharing is conducted "in accordance with this title."[56] This provision pulls in all of CISA's information sharing requirements, including two provisions that private entities need to consider. First is the requirement discussed above that the private entity remove information that it "knows at the time of sharing" is personally identifiable and not "directly related" to the threat.[57] In other words, if a private entity knowing shares private data not related to the threat, it potentially could be subject to third-party liability. Second, a *receiving* entity must comply with "otherwise lawful restrictions placed on the . . . *use* of such [information] *by the sharing non-Federal entity*."[58] This second provision is interesting as it raises the possibility that a private entity sharing threat indicators with another private could do so subject to contractual restrictions, then sue the receiving entity for violating them.

---

[51] *Id.*
[52] CISA § 105(c)(1), (c)(1)(B) ("[T]he Secretary of Homeland Security . . . shall develop and implement a capability and process . . . that . . . shall . . . be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title . . . .").
[53] INTERIM GUIDELINES, *supra* note 40, at 7.
[54] DEPT. HOMELAND SECURITY & DEPT. OF JUSTICE, GUIDANCE TO ASSIST NON-FEDERAL ENTITIES TO SHARE CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH FEDERAL ENTITIES UNDER THE CYBERSECURITY INFORMATION SHARING ACT OF 2015 at 12 (2016).
[55] Id. § 104(c)(1) ("[A] non-Federal entity may, for a cybersecurity purpose . . . share with or receive from any other non-Federal entity . . . a cyber threat indicator or defensive measure.")
[56] *Id.* § 106(b)(1).
[57] *Id.* § 104(d)(2)(A).
[58] *Id.* § 104(d)(c)(2) (emphasis added).

Participation

Nothing in CISA makes participation mandatory. No private entity is required to share information with any other entity or with the federal government.[59] Congress further underscores this point by providing that CISA does not create any duty to share information or to warn about cyber threats.[60]

Thus, private entities need to consider the benefits and drawbacks of sharing information under the CISA framework. What those benefits may be is yet to be determined; business will need to wait and see what processes and procedures DHS ultimately develops in order to determine whether the benefits exist or, as CISA critics have charged, if they are ephemeral.

Such benefits, however, would need to be weighed against the risk of backlash from customers and other stakeholders in the company. CISA permits the use of data shared with the government for law enforcement purposes that are unrelated to cybersecurity.[61] Even if it turns out that CISA does little to compromise personal privacy, it is not unforeseeable that customers, employees, and business partners could rebel against a company that is perceived as sharing their data with the government. As the Sony hack illustrated, significant reputational damage can result from private company data entering the public realm, even if that data is not strictly personally identifiable.[62] It is not unimaginable that sharing between private entities under CISA could lead to similar scandal, and therefore it may be wise to take a wait-and-see approach.

Conclusions

CISA 2015 represents significant progress in that Congress was able to pass legislation to improve cyber security. Optimistically, the implementation of this legislation will actually meet this goal, and DHS and DOJ have just released the guidance for non-Federal entities on how to share information with the Federal Government. Additionally, on February 9, the White House issued the "Cybersecurity National Action Plan," calling for "partnerships between Federal, State and local government and the private sector in the development, promotion and use of cybersecurity technologies, policies, and best practices."[63] Threat intelligence sharing should fall under this umbrella. All actors in this system, however, must continue to be cognizant of individual privacy. There is a legitimate criticism of CISA that it does not do enough to protect the privacy of users, and therefore it may be up to private

---

[59] Note, however, that some CISA critics have charged that the program may be technically voluntary but could end up being so coercive that private entities are forced to participate so as not to be at a competitive disadvantage. *See* Amie Stepanovich, *Busting the Biggest Myth of CISA—That the Program Is Voluntary*, WIRED Aug. 8, 2015.
[60] *Id.* § 106(c).
[61] For example, information shared with the government can be used for "preventing or mitigating[] a serious threat to a minor, including sexual exploitation," as well as various criminal fraud and espionage statutes. See id. § 105(d)(A).
[62] *See* Dominic Rushe, *Amy Pascal Steps Down from Sony Pictures in Wake of Damaging Email Hack*, GUARDIAN, Feb. 5, 2015, *available at* http://www.theguardian.com/film/2015/feb/05/amy-pascal-leaving-sony-pictures-email-leak (last visited Feb. 10, 2016).
[63] https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

industry to step into the breach and go the extra mile that is not required in order to protect its customers and customer relationships.

Consideration of the points discussed here will help with implementation of this process and the companion process for sharing by the Federal government. If Congress and the Executive branch can work together while keeping in mind the changing needs of private organizations, we can reduce the cyber risks that we all face.

Jason R. Edgecombe *is an attorney with Baker, Donelson, Bearman, Caldwell & Berkowitz, PC in Atlanta, Georgia. As part of the firm's Privacy and Information Security and its Government Enforcement and Investigations practices, Jason represents clients facing enforcement issues with federal and state governmental bodies arising out of data security incidents, as well as civil litigation arising from such events. Jason received his B.A. from Emory University and his J.D., with high honors, from Emory University School of Law, where he served as the Executive Managing Editor of the Emory Law Journal. Jason is a member of the International Association of Privacy Professionals (IAPP) and the American Bar Association (ABA).*

Dr. Frederick Scholl *is President of Monarch Information Networks, where he provides security risk assessments to US and global clients and provides expert witness testimony in cases involving security best practices and security intellectual property. He is also teaching information security at Vanderbilt University and Lipscomb University, both in Nashville, TN. He is a member of the ABA ISC, ISSA, ISACA and SIM.*

Biometric Collection: A New Era of Technology and Privacy Concerns

By Ashley L. Thomas

"If someone hacks your password, you can change it – as many times as you want. You can't change your fingerprints. You have only ten of them. And you leave them on everything you touch." Senator Al Franken.[1]

Companies are making concerted efforts to ramp up cybersecurity efforts but it appears that hackers are not always far behind overcoming those security efforts. In an effort to use alternative means of security, companies are turning to biometric identification to make financial transactions more efficient and potentially harder to hack given the unique identification biometric information can offer. There are numerous ways companies are using biometric identification such as unlocking a software program by providing a fingerprint or scanning faces in a retail store by using facial recognition technology to identify potential shoplifters. However, the law governing the use and collection of biometric information isn't well defined.

This article will explore the developing legal framework surrounding biometric information by examining state laws that have been adopted to regulate biometric information privacy and recent cases filed challenging these laws.

Background on Biometric Information

Biometric information includes physiological data such as retina or iris scans, fingerprints, heat signatures, facial geometry scans as well as behavioral data such as handwriting samples and voice prints. These identifiers are typically used for authentication or identification purposes. There are currently no federal laws that limit a private entity's ability to collect, use or disclose biometric information.

The Federal Bureau of Investigation ("FBI") and other law enforcement agencies with the help of facial recognition technology have slowly been amassing collections of "faceprints," to track criminals and prevent identity fraud. Faceprints, sometimes called facial templates, are developed by software programs that automatically convert distinguishing features of every face in a photo into a unique mathematical code. This code can then be applied to future photographs in order to identify individuals within the photograph. Companies such as Facebook and Google Plus have developed face recognition software that automatically identifies and tags the user and their friends in photographs. In 2013, Facebook acquired an Israeli facial recognition technology company called Face.com for $100 million to enhance mobile recognition for users on the go. With this acquisition Facebook rolled out

[1] Letter from Sen. Al Franken, Chairman of the Senate Committee on Judiciary to Tim Cook, CEO of Apple, Inc., (Sept. 19, 2013) (available at http://www.franken.senate.gov/files/documents/130919AppleTouchID.pdf).

what they call "DeepFace" technology, a facial alignment system based on explicit 3D modeling of faces. According to a Facebook research group this facial recognition technology allegedly reaches an accuracy of 97.35% closely approaching human-level accuracy.[2] Social media websites. Facebook's facial recognition software is reported to be more accurate than the FBI's, Next Generation Identification program.[3] Facebook withdrew their photo tagging feature from the European Union after an audit report was released by Irish regulators finding the feature to be invasive.[4]This has caused concern because some privacy advocates believe that faceprints are a unique biometric identifier that requires an individual's consent before companies can collect and share this information. Facial recognition technology also raises concerns of its effect on each person's ability to remain anonymous in public such as on a sidewalk or in a store as well as the capability to track individuals across geographic locations. Senator Al Franken has stated that "there is nothing inherently right or wrong with [facial recognition technology, but] if we do not stop carefully and consider the way we use [it], it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties."[5] Senator Franken further notes that facial recognition technology could be "abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution."[6]

FTC Best Practices on Facial Recognition Technology Use

The Federal Trade Commission ("FTC") compiled a report on best practices for companies to consider when using facial recognition technology.[7] The report provided two scenarios in which companies should obtain express consent before using or collecting consumer's faceprints. Companies should obtain consumer consent before using any image or biometric data derived from that image in a materially different manner than the company represented when they collected the data. Also, companies should avoid using facial recognition technology to identify anonymous images of a consumer to someone who could not otherwise identify that individual unless the consumer has given authorization. The report gave the example of a mobile app that allows the user to identify strangers in public places by simply taking a photograph of the stranger and uploading it to the app to search their database. Users could learn that stranger's identity and possibly more information such as an address. The FTC acknowledged that this example raises significant privacy concerns and the mobile should only

---

[2] Taigman, Yaniv, et. al. *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*, (available at https://research.facebook.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/)

[3] Brandom, Russell, *Why Facebook is Beating the FBI at Facial Recognition*, THE VERGE, (July 7, 2014), (available at http://www.theverge.com/2014/7/7/5878069/why-facebook-is-beating-the-fbi-at-facial-recognition).

[4] Re-Audit Report by Facebook, (Sept. 21, 2012) https://www.dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf

[5] *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the Senate Committee on Judiciary*, 112th Cong. 1 (2012) (available at http://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf)

[6] *Id*.

[7] *Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies*, Federal Trade Commission (Oct. 2012), *available at* https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf.

identify those individuals who have consented to participate with this application. Additionally, the FTC urged social media sites that utilize facial recognition technology should consider adopting protections that would "prevent unauthorized scraping of the publicly available images it stores in its online database."[8] Social network sites should establish and maintain appropriate retention and disposal practices of biometric data." The FTC provided the example of Google Plus's "My Face Feature" that suggests photo tags of other users that have consented to the feature by turning it on. If the user no longer wishes to use this feature, the user can simply turn it off which deletes the biometric data collected from that user.

State Laws on Biometric Information

While companies are racing to adopt biometric security measures, few states have enacted statutes to address privacy and security concerns with biometric information. Illinois and Texas are the leading states to have adopted measures to monitor private entities use and collection of biometric information. The Illinois Biometric Information Privacy Act[9] (BIPA) was adopted in response to the growing use of biometric identifiers in the business and security screening sectors in an effort to streamline financial transactions. Illinois recognized that biometrics are unlike any other unique identifiers used to access financial or other sensitive and when this data is compromised the individual has no recourse. This heightened risk for identity can force some individuals to withdraw from biometric-facilitated transactions. Under BIPA, private entities have to inform users in writing: (1) that their biometric information is being collected and/or stored and(2) the specific purpose of the biometric data collection and length of time the biometric data will be stored. Once a user has been informed, this individual must provide a written release giving their consent to the biometric data collection.

BIPA also requires that private entities in possession of biometric information must develop a written policy that establishes a schedule retaining and guidelines for permanently destroying biometric information. In addition, private entities are prohibited from selling, trading or otherwise profiting from an individual's biometric information. BIPA provides statutory damages of $1,000 per negligent violation and $5,000 for intentional or reckless violations and permits a greater recovery if actual damages exceed the liquidated damages amount. Texas adopted a biometric privacy act with similar provisions of the Illinois law but only the attorney general can bring an action against a company collecting this data.[10] A person who is found in violation of the Texas law is subject to a civil penalty of $25,000 for each violation.

[8] *Id*.
[9] 740 ILCS 14/5.
[10] Tex. Bus. & Com. Code Ann. § 503.001.

Facial Recognition Technology Lawsuits

Facial recognition technology software and the collection of biometric information has been the point of contention for class action lawsuits filed against popular social media site, Facebook and Shutterfly, a photo-book service.

A class action lawsuit was filed against Shutterfly and its subsidiary ThisLife.Com, Inc. in June 2015 claiming the company violated BIPA because it collected and stored facial templates of non-members without obtaining their permission.[11] Shutterfly users have stored approximately 20 billion photos in the company's database. The lead plaintiff, Brian Norberg, who is not a Shutterfly subscriber, alleges that when a user uploaded an image of Norberg, Shutterfly automatically scanned and analyzed Norberg's face and extracted the points and contours of his face creating a unique face template. The user then tagged Norberg in the image and Shutterfly stored Norberg's face template in their database.

The face template was also used by Shutterfly to recognize Norberg's gender, age, race and location. Norberg never gave his consent to Shutterfly to collect and store his biometric information which he claims is a direct violation of BIPA. Shutterfly filed a motion to dismiss the lawsuit arguing that the definition of "biometric identifier" under BIPA expressly excludes photographs and that "biometric information" does include information extracted from photographs. According to Shutterfly, the lawsuit should be dismissed because BIPA was applicable to their facial recognition technology. On December 29, 2015, a federal judge in the Northern District of Illinois disagreed with Shutterfly and denied the motion to dismiss finding that Norberg plausibly stated a claim for relief under BIPA.[12] The judge acknowledged that the court was unaware of any previous judicial interpretation of the statute. The case will move forward with the possibility that additional class actions might be filed.

Facebook is currently facing several class action lawsuits with plaintiffs alleging, similarly to Shutterfly, that Facebook is illegally collecting and storing biometric data. In one class action suit, *Licata v. Facebook, Inc.*, the case has been transferred to the Northern District of California.[13] Facebook filed a motion to dismiss arguing that BIPA isn't applicable because of the choice of law provision in Facebook's terms of service citing California law as the standard to follow. California currently doesn't have a biometric privacy act. In another class action lawsuit, *Gullen v. Facebook, Inc.*, moved to dismiss the case citing lack of personal jurisdiction and failure to state a claim.[14] However, that case was dismissed for lack of personal jurisdiction. The federal judge did not decide whether Gullen failed to state a BIPA claim but considered it moot.

---

[11] *Brian Norberg v. Shutterfly Inc., et al.*, Case No. 1:15-cv-05351 (N.D. Ill. 2015) (available at http://www.scribd.com/doc/269046832/Shutterfly-Class-Action-Complaint#scribd).
[12] *Brian Norberg v. Shutterfly Inc., et al.*, No. 15-05351 (N.D. Ill. Dec. 29, 2015)) (available at http://www.scribd.com/doc/294580365/NorbergVShutterfly-Order-on-Motion-to-Dismiss-12-29-15).
[13] *Licata v. Facebook, Inc.*, No. 15 CH05427 (Ill. Cir. Ct. Cook Cty. filed Apr. 1, 2015).
[14] *Gullen v. Facebook, Inc.*, No. 15 C 7681 (N.D. Ill. January 21, 2016) (available at https://scholar.google.com/scholar_case?case=2347505145568090007&hl=en&as_sdt=6&as_vis=1&oi=scholarr)

Conclusion

During the summer of 2015, the American Civil Liberties Union (ACLU) and the Center for Democracy and Technology along with seven other civil liberties and consumer advocacy groups withdrew from the National Telecommunications and Information Administration initiative talks.[15] These advocacy groups were negotiating with industry trade groups to establish commercial guidelines for the use of facial recognition technology. However, the advocacy groups withdrew from the talks on a lack of consensus related to a minimum standard of consent. It is unclear whether the FTC will step in to regulate and issue any further or binding guidance on the use of facial recognition technology. In the meantime, private companies should review the FTC's best practices report and evaluate their companies policies and procedures in the collection and storage of biometric information. Companies doing business in Illinois and Texas should carefully review their policies and procedures on the collection of biometric to ensure the company is complying with their specific state requirements.

Ashley Thomas *is an associate in the Indianapolis office of Hall, Render, Killian, Heath & Lyman. She practices in the area of healthcare law with a focus on hospital and health system matters, regulatory and compliance issues, and health information privacy and security. Ms. Thomas received her J.D from Vanderbilt University Law School and her B.A. in Political Science from Northwestern University. She may be reached at athomas@hallrender.com*

[15] Singer, Natasha, *Consumer Groups Back Out of Federal Talks on Face Recognition*, N.Y. TIMES BLOG (June 16, 2015) (available at http://bits.blogs.nytimes.com/2015/06/16/consumer-groups-back-out-of-federal-talks-on-face-recognition/).

EU's General Data Protection Regulation – What Does It Mean for Business?

By Kate Colleary

After many years of negotiation, consulting, drafting and even a movie made about it,[1] on 15 December 2015, the European Parliament, Commission, and Council of Ministers reached agreement on the text of the General Data Protection Regulation ("GDPR"). This draft is likely to be formally adopted in spring 2016. There will then be a two-year period following which the GDPR will become directly applicable in all European Union ("EU") member states.

The GDPR will replace the EU Data Protection Directive[2] and there are some significant changes to the existing legislative framework which we have highlighted below. Businesses should begin to prepare now to ensure compliance.

What does it mean for business?

1. **A "one-stop shop"**

One of the most significant changes under the GDPR is that companies will be regulated by one lead Supervisory Authority[3]. The GDPR provides that the lead supervisory authority for any undertaking will be dependent upon that undertaking's place of main establishment. In practice, this means that where a data controller or data processor has a number of establishments within the EU, the supervisory authority of the member state where the data controller/processor has its "main establishment" will be the authority that supervises and enforces its data protection compliance across the EU. The "main establishment" of a data controller in the EU should be the place of its central administration in the EU unless decisions relating to the purposes and means of processing personal data are taken elsewhere in the EU.[4]

This one change will revolutionise the process by which data protection law is regulated in the EU. However, following protracted negotiations, the "one-stop-shop" principle has been somewhat watered down by the requirement for the lead supervisory authority to consult and cooperate with other, "concerned" supervisory authorities. Each supervisory authority should be competent to deal with local cases where the subject matter of the processing concerns only processing carried out in a single member state and involving only data subjects in that single member state. In that case, the lead supervisory authority will be notified and will decide whether to deal with the case on a "one stop shop" basis under Article 54 (a) or at local level by the local supervisory authority. Furthermore only local

[1] Democracy – a 2015 film by David Bernet documenting the negotiation and finalisation of the GDPR
[2] 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
[3] Article 51(a) Draft GDPR
[4] Recital 27 and Article 51(a) Draft GDPR

supervisory authorities will deal with issues relating to their national public authorities or private bodies acting in the public interest.

The GDPR creates a European Data Protection Board ("EDPB") which will be made up of one representative of each EU member state's supervisory authorities and a representative of the European Commission. It may issue binding decisions which are subject to appeal to the Court of Justice of the European Union ("CJEU"). However various commentators are concerned that the efficacy of the GDPR, may be hindered by the potential for multiple references being made to the EDPB and, indeed, appeals to the CJEU. Whatever the outcome in practice, these are some very significant new administrative and procedural changes to the European Data Protection framework.

Given the introduction of a one-stop shop regulator, we are likely to see large, data-centric, multinational companies '"regulator–shopping" ie choosing their place of main establishment not just based on tax advantages or physical location but also by the attitude of the local supervisory authority. Multinational businesses should consider the attitude of the data protection supervisory authority in various member states when deciding where to locate their place of main establishment in the EU. Furthermore, it will be critical for multinational companies to develop a good working relationship with their lead supervisory authority.

2. Risk Analysis and Privacy by Design and Default

The GDPR adopts a risk-based approach to data protection regulation. This means that some compliance obligations will only apply to data processing activities that are likely to result in a risk to an individual's data protection rights. This is reflected in the obligation to notify supervisory authorities and individuals of data breaches where there is a risk to the individual's data and to carry out privacy impact assessments. The GDPR also places significant emphasis on adopting appropriate policies and implementing the safeguards to protect personal data.[5]

Privacy should be a paramount consideration in any processing activity carried out by a business. Appropriate technical and organisational measures must be drafted, adopted and implemented both prior to and during the data processing, to ensure compliance with data protection principles[6]. A key term used throughout the draft GDPR is transparency – businesses should seek to be clear and transparent in their dealings with individuals.

Where a type of processing is likely to result in a high risk for the privacy of individuals, a data controller must carry out a Privacy Impact Assessment ("PIA")[7], i.e. evaluate the risks and assess how they can be limited. Whenever a Privacy Impact Assessment demonstrates that there is a high risk for data subjects, the data controller must inform its lead supervisory authority to obtain its view on the

[5] Recital 61 and Article 22(2)(a) Draft GDPR
[6] Article 23(1) Draft GDPR
[7] Recital 66a and 74 and Article 33 Draft GDPR

processing activity and the data controller's proposed risk mitigation measures[8]. The supervisory authorities must establish and publish a list of the kind of processing operations which will require a PIA to be carried out[9]. As a matter of practicality, the PIA concept must be integrated within businesses' policies and procedures. We would also recommend that businesses establish PIA training programs so that those responsible for data processing activity in the business will understand when and how PIA's should be carried out. Furthermore, it is important to document the policies and processes that relate to carrying out PIA as well as documenting the PIA itself.

One element of the GDPR that has received significant attention is that certain categories of businesses will be required to appoint a Data Protection Officer to oversee compliance with data protection law[10]. Any organisation which regularly or systemically gathers data as part of its core activities and any data controllers or data processors who process large amounts of sensitive personal data will be required to appoint a Data Protection Officer ("DPO"). The DPA may be an employee of the data controller and may fulfil other tasks or duties as long as there is no conflict of interest with his/her role as DPO. The role of DPO may also be outsourced and must be independent.[11]

The current system of submitting routine notifications to the relevant supervisory authority has been abolished in favour of a privacy by design/policy based approach[12]. Instead, both data controllers and processors will need to keep internal records of the processing which they carry out – including the names and contact details for data processors, controllers and joint controllers[13]. There is an exemption from these documentation requirements for SMEs – organisations who employ less than 250 people. The SME exemption will not apply if the organisation engages in risky processing, processing of special categories of data[14]; data about criminal convictions or where the processing is "not occasional."

3. Pseudonymisation

The GDPR introduces the concept of 'pseudonymisation'. While many companies carry this out in practice already, the GDPR encourages its use to enhance data subjects' privacy rights. Essentially, 'pseudonymisation' involves personal data being partially anonymised i.e. two datasets are maintained, one with the individual's identifying information and the other with an identifying marker. The two datasets are held separately and subject to technical and organisational measures to ensure non-attribution.

---

[8] Article 33 Draft GDPR
[9] Article 33(2)(a) Draft GDPR
[10] Recital 75 and Article 35 Draft GDPR
[11] Article 35(8) Draft GDPR
[12] Recital 70 Draft GDPR
[13] Recital 65 and Article 28 Draft GDPR
[14] The references to "sensitive personal data" Under the Data Protection Directive have been replaced with "special categories of data as set out in Article 9(1) Draft GDPR

4. Consent

Under the GDPR, consent should be given by a clear affirmative action establishing a freely given, specific, informed and unambiguous agreement to the processing[15]. Importantly, consent must be specific to the purpose for which the data has been collected. If any additional processing is to be carried out and such processing is incompatible with the original purpose, fresh consent must be obtained. Furthermore, inaction (opt-out) is not an acceptable form of consent under the GDPR and consent must be proactive i.e., "opt-in"). This is reflected by the requirement for a "clear affirmative action."

The age of consent is 16, unless member state law provides for a younger age of consent which cannot be below 13.[16]

5. Outsourcing to Data Processors

Under the current data protection regime, a data controller that outsources its data processing activity remains responsible for anything that happens to that data while it is being processed by the third-party data processor. The Data Protection Directive places limited obligations on data processors and only requires that data processing agreements are in writing and there are no further requirements in relation to the terms of the agreements. However, under the draft GDPR, data processors will assume additional responsibility in some areas, such as data transfers[17]. Furthermore, approval must be sought from data controllers to allow data processors appoint sub-processors and to transfer data out of the European Economic Area. The GDPR also recognises the data controller's right to carry out audits on the data processor.

6. Some New Rights

Right to be Forgotten

The GDPR introduces an explicit right to be forgotten[18]. This means that, under certain circumstances, eg if the retention of the data is not in compliance with the GDPR; the data is no longer needed or consent is withdrawn, personal data must be erased "without undue delay." How this will operate in practice and, in particular, the extent of the potentially significant administrative burden this places on businesses has yet to be established.

[15] Recital 25 Draft GDPR
[16] Article 8 Draft GDPR
[17] Article 26 Draft GDPR
[18] Recital 53 and Article 17 Draft GDPR

Data portability[19]

Where data is being processed by automated means, eg where individuals have provided personal data to a cloud storage provider, the GDPR provides the individuals with a right to transmit the data to another service provider. This right is contingent upon this being technically feasible.

Automated decision-making

The GDPR restricts a data controllers' ability to engage in entirely automated-decision-taking, if the decision could produce legal effects or significantly affect the data subject[20]. The data subject also has a right to object to such data processing. If a controller wishes to engage in entirely automated–decision–taking, appropriate protections for the data subject must be put in place. If the processing is based on the data subject's consent or is necessary to enter into, or to perform, a contract then the data subject will not have a right to object to the processing but will have a right of human intervention and appeal. Automated decisions involving special categories of data are further restricted.[21]

7. Data Breaches

Under the GDPR, undertakings must notify their Supervisory Authority within 72 hours of becoming aware of a data breach unless the breach is unlikely to result in a risk for the rights and freedoms of individuals[22]. This is likely to become an interesting topic for judicial interpretation and may be difficult to enforce and it is quite subjective. It is likely that guidance will issue on this point. Further, the individuals affected must be notified if it the breach is likely to result in a "high risk to the rights and freedoms of individuals" and the data is not encrypted and such notice must be provided "without undue delay.[23]"

There is no obligation to report a breach which is unlikely to result in a risk to individuals. However, undertakings must still retain a record of breaches, so that Supervisory Authorities can assess compliance during a later audit or investigation.

8. Jurisdictional issues

The GDPR will apply whenever personal data is processed in connection with the offer of goods or services to EU citizens or where data subjects' behaviour within the EU is being monitored[24]. This will be the case regardless of where the data controller/processor is based, even if the business processing the personal data has no EU presence. This has significant repercussions from multinational undertakings based outside the EU, offering goods or services into the EU. Data processing activities

[19] Recital 55 and Article 18 Draft GDPR
[20] Article 20 Draft GDPR
[21] Article 20 (3) Draft GDPR
[22] Recital 67 and Article 31 Draft GDPR
[23] Article 32 Draft GDPR
[24] Article 3 Draft GDPR

carried out by these undertakings will be covered by the GDPR, and subject to the significant fines for non-compliance. Furthermore, where a business has no place of establishment within the EU, but where it supplies services to or monitors EU data subjects, it will need to appoint a representative in the EU[25] unless its processing is "occasional" and does not include large scale processing of special categories of data or certain other processing activity as set out in the GDPR.

9. Financial Penalties and Damages

The national Supervisory Authorities will be granted the ability to impose monetary fines on data controllers and data processors. The maximum fine will be 4% of an undertaking's total worldwide annual turnover in the previous year. Similar to the situation under the current regime, individuals will also be entitled to claim compensation for any damage caused to them by the actions of the data controller. However this remedy has been extended to include data subjects taking action against data processors for breach of those provisions of the GDPR which are directed to processors, or if they act outside the lawful instructions of the controller.

In these cases, the burden of proof will lie on the data controller/data processor to prove that they are not responsible for the event which has caused the damage.

10. Transfers of Data

Existing methods for transferring personal data continue to be recognised under the GDPR.[26] Model EU contractual clauses may still be used. However, following the case brought by Max Schrems,[27] the "safe harbour" system for transferring data to the US is being re-negotiated. At the time of writing (2 February 2016), an agreement has just been reached with regard to the terms of a second safe harbour arrangement – a US Privacy Shield. Details are awaited as to the terms of the agreement. Furthermore, companies transferring data to the US based on EU model clauses may also have their arrangements reviewed to determine whether the transferee country (i.e. the US) has sufficient safeguards in place to protect EU citizens' data. Despite these developments, the current draft wording of the GDPR provides that:-

1. Existing authorisations for Binding Corporate Rules will remain valid.[28]
2. Contracts incorporating standard EU Model clauses remain in operation.
3. Transfers may be permitted based on approved codes of conduct or certifications issued under a newly introduced scheme,[29] provided that binding and enforceable

[25] Article 25 Draft GDPR
[26] Recitals 19,20 and 21; Articles 41, 42 and 43 Draft GDPR
[27] Case C-362/14 Request for a preliminary ruling under Article 267 TFEU from the High Court (Ireland), *Maximillian Schrems v Data Protection Commissioner*
[28] Article 43 Draft GDPR
[29] Articles 38 and 39 Draft GDPR

commitments are made by the data controller or processor to apply the appropriate safeguards.

4. The GDPR provides that it is not lawful to transfer personal data out of the EU in response to a legal requirement from a third country.[30]

Next Steps

One of the common themes in the GDPR is that of standardisation. We are seeing the introduction of standardised data processing contracts[31]; certification standards[32]; approved codes of conduct[33]; and standardised icons for notifications to data subjects.[34]

Now is the time for businesses to prepare for the implementation of the GDPR. Once enacted, the GDPR will apply directly in each of the 28 EU member states. It will not only apply to the data processing activities of EU businesses but also to data processing activities of any business, regardless of location, that target EU data subjects. This means that regardless of where a business is based, if it provides services to, or targets EU data subjects, it will be required to comply with the GDPR, or else face the very significant fines for non-compliance.

While the high level of fines and the introduction of some new data subject rights appeared to change the data protection landscape under the GDPR, its objective is not dissimilar from the current Data Protection Directive and the fundamental principles as set out in article 5 of the Draft GDPR are essentially the same as under the Directive. This means that if businesses are compliant with the current regime, it should not require significant time, cost or energy to adapt their policies and procedures to comply with the GDPR. The key issue is to ensure that data protection is enshrined in all processing activities carried out by the business - privacy by design – and that the appropriate policies and procedures are in place.

Many larger companies are considering appointing a Data Protection Officer now to manage data protection issues in the business and to highlight any areas of concern prior to the enactment of the GDPR. The appointment of a DPO will be a requirement under the GDPR for some companies, so they may as well gain the advantage of picking the brightest and the best early, and so that that person can be instrumental in crafting the businesses GDPR compliance plan.

---

[30] It will be interesting to see how the awaited judgment the Microsoft case in the US interacts with this element of the GDPR

[31] Article 26(2)(b) Draft GDPR

[32] The Draft GDPR provides for Data Protection certification seals/marks which may be approved by a certification body (Article 39a); a supervisory authority (Article 43a) or the EDPB (Article 57). The certification seals will run for three years and may be renewed. A list of the recipients of the seals will be collected by the EDPB and kept on a publically available register.

[33] Article 38 Draft GDPR provides for a code of conduct to be approved by a supervisory authority, or under the Article 57 procedure by the EDPB. If sent to the EDPB, the Commission may approve the code and all codes will be collected and kept by the EDPB on a publically available register.

[34] Article 14 and 14a Draft GDPR

While the amount of coverage of the negotiation of the GDPR is unprecedented for a piece of European legislation, the fundamentals have not changed terribly. To achieve compliance, concentrate on getting your business' processes and procedures correct and in the immortal words of Douglas Adams – "Don't panic"!

Kate Colleary *specialises in Intellectual Property, Data Protection, Commercial and Litigation work. For sixteen years she worked in large international practices in Dublin, most recently heading up the Intellectual Property and Data Protection groups of an International law firm. Kate set up Colleary and Company as a boutique law firm to provide clients with top quality advice and service, with a personal touch.*

The New Year Brings Changes to Proportionality and Sanctions Rules

By Khadijah Robinson, Alexander Hastings, and Edward Rippey

E-discovery can be an extraordinarily expensive and time-consuming process, especially when preserving, collecting, and reviewing electronically stored information ("ESI").[1] *In response to ongoing concerns regarding these burdens, the Advisory Committee on Rules of Civil Procedure (the "Committee") proposed several changes to the Federal Rules of Civil Procedure, which became effective on December 1, 2015. The two most significant amendments for e-discovery appear in* Rule 26(b)(1), which limits the scope of discovery, and Rule 37(e), which concerns e-discovery sanctions. Regarded by some as the "most significant changes to discovery in the past 25 years," the amendments could have a significant impact in the e-discovery community.[2] This article reviews these amendments and discusses how they may address persistent problems faced by e-discovery practitioners.

I. Rule 26: The Scope of E-Discovery and the Principle of Proportionality

Although some maintain that the previous version of Rule 26(b) served as an "invaluable resource for limiting the scope of e-discovery,"[3] many e-discovery practitioners realized that the rule in practice provided slight relief in light of the sheer volume and scope of many discovery requests. Indeed, courts often declined, expressly or implicitly, to invoked the proportionality principle.[4] Therefore, when amending Rule 26(b), the Committee emphasized that it intended to make it "clear…to the courts and litigants that pretrial discovery is subject to inherent limitations."[5] To this end, the Committee shifted the provision that allows courts to limit overly expansive discovery requests from Rule 26(b)(2)(C)(iii) to the center of the discussion of the scope of discovery at Rule 26(b)(1).

The quotation below illustrates the amendment, with the new language underlined and the prior language struck:

---

[1] Steven C. Bennett, *E-Discovery: Reasonable Search, Proportionality, Cooperation, and Advancing Technology*, 30 J. Marshall J. INFO. TECH. & PRIVACY L. 433, 438 (2014).
[2] Betsy Barry et. al., *The Big Esi: Going from Big to Better in E-Discovery*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 721, 733 (2015).
[3] Kevin A. Griffiths, *The Expense of Uncertainty: How A Lack of Clear E-Discovery Standards Put Attorneys and Clients in Jeopardy*, 45 IDAHO L. REV. 441, 475 (2009)
[4] Defining the Problem of Cost in Federal Civil Litigation, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1486&context=dlj. But see *Moore v. Publicis Groupe*, 287 F.R.D. 182, 186 (S.D.N.Y. 2012) adopted sub nom. *Moore v. Publicis Groupe SA*, No. 11 CIV. 1279 ALC AJP, 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012) (disallowing the plaintiff's request for information from additional data sources without providing additional information in compliance with Rule 36(b)(2)(C)).

(b) Discovery Scope and Limits.

(1) *Scope in General.* Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable. ~~— including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C)~~.

This amendment returns the proportionality language to where it once appeared in the 1983 version of the Rules,[6] underscoring that proportionality is no longer a back-end consideration, but rather part of the definition of the scope of discoverable information—that is, ESI is discoverable when it is relevant *and* proportional.

The Committee made several additional changes to Rule 26's language:

- To address potential issues related to one party having greater access to relevant documents and information, the Committee added a factor for considering "the parties' relative access to relevant information."[7]

- In a small but meaningful edit, the Committee reversed the order of the factors for the "amount in controversy" and the "importance of issues at stake in the action." By placing the "importance of issues" first in the list of considerations, the Committee intended to highlight that cost may not be the controlling factor in determining the proportionality of an e-discovery request.[8]

- The Committee added the factor of "whether the burden or expense of the proposed discovery outweighs its likely benefit" to demonstrate the strong desire to return proportionality to the judicial consciousness.[9]

[6] FED. R. CIV. P. 26(b), Advisory Committee's Note (2015 amendments).
[7] *Id.*
[8] *Id.*
[9] *Id.*

- The Committee removed the provision allowing for the discovery of relevant but inadmissible information that appears "reasonably calculated to lead to the discovery of admissible evidence."[10] The Committee noted that litigants had wrongly relied on this phrase to seek overly broad discovery.[11]

- Although the Committee deleted the enumerated examples of discoverable information (e.g., the existence, description, nature, etc., of documents) from the Rule, the Committee notes that this change was simply a space-saving measure and that these examples are still applicable.[12]

- The Committee deleted the clause authorizing the court, for good cause, to order discovery of any matter relevant to the subject matter involved in the action, noting that "this language is rarely invoked."[13]

II. Sanctions for Spoliation of Evidence

The stakes for missteps in e-discovery, whether intentional or inadvertent, can be very high. For instance, in one case, the court not only struck the defendant's answer, dismissed its counterclaims with prejudice, entered default judgment for the plaintiff, and imposed monetary sanctions, but also referred the case to the U.S. attorney for criminal prosecution of discovery abuses.[14] Given these high stakes, parties have expressed concern for years regarding the inconsistent standards for imposing sanctions, especially as the inconsistency relates to the level of culpability required. Indeed, some courts found mere negligence sufficient to impose sanctions for spoliation of ESI, sanctioning litigants whose spoliation was simply the result of an existing policy of periodically destroying ESI.[15] On the other hand, some courts have required gross negligence, willfulness, or bad faith,[16] while still others require a "culpable state of mind" without defining what degree of culpability is necessary.[17]

---

[10] *Id.*

[11] *Id.* In comments to the Committee regarding the proposed rules, we advanced the argument that this clause should be removed, as he has repeatedly experienced parties relying on the reference to information being "reasonably calculated to lead to" admissible evidence to support overly broad discovery. *See* Letter from Covington & Burling LLP to Advisory Committee on Civil Rules 5–6 (Feb. 13, 2014), http://www.regulations.gov/#!documentDetail;D=USC-RULES-CV-2013-0002-1157

[12] FED. R. CIV. P. 26(b), Advisory Committee's Note (2015 amendments).

[13] *Id.*

[14] *See Philips Elecs. N. Am. Corp. v. BC Tech.*, 773 F. Supp. 2d 1149, 1216 (D. Utah 2011).

[15] *See, e.g.*, *Medcorp, Inc. v. Pinpoint Techs., Inc.*, No. 08–cv–00867, 2010 WL 2500301, at *3 (D. Colo. June 15, 2010) (imposing monetary sanctions when "Defendants have not established that Plaintiff has violated any discovery order in this case, and there is no substantial evidence that its destruction of hard drives or the recycling of its workstations was anything other than what Plaintiff would do in the ordinary course of business" (internal modifications omitted)).

[16] *See, e.g.*, *Sherman v. Rinchem, Co.*, 687 F.3d 996, 1006–07 (8th Cir. 2012) (affirming a lower court's decision not to grant sanctions in absence of bad faith); *Saenzpardo v. United Framing Constr. Co.,* No. 10-00049-CG-M, 2011 WL 5037414, at *2 (S.D. Ala. Oct. 21, 2011) (explaining that mere negligence does not qualify as the bad faith level of culpability required for an adverse inference instruction in the Eighth Circuit).

[17] *Painter v. Atwood*, No. 2:12-CV-01215-JCM-RJJ, 2014 WL 1089694, at *8 (D. Nev. Mar. 18, 2014) ("The party seeking an adverse inference instruction must establish: (1) that the spoliating party had an obligation to preserve the evidence; (2)

Additionally, once the level of culpability for imposing sanctions is established, there has been much variation among courts as to the appropriate sanction at each level of culpability. For instance, some courts have permitted negligent conduct to lead to an adverse inference, while others require intentional conduct or bad faith.[18]

These varying approaches arose, in part, from Rule 37(e)'s former safe harbor provision and the federal courts' ability to use their inherent authority to issue sanctions for spoliation without reference to the Rules. The new Rule 37(e) seeks to resolve the inconsistencies.[19] The quotation below illustrates the amendment, with the new language underlined and the prior language struck:

(e) Failure to Provide Preserve Electronically Stored Information. ~~Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.~~ If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

---

that the evidence was destroyed or significantly altered with a culpable state of mind; and (3) that the evidence was relevant to the other party's claim in that a reasonable trier of fact could find that it would support that claim.").

[18] *Compare Medeva Pharma Suisse A.G. v. Roxane Labs., Inc.*, No. 07-5165 (FLW), 2011 WL 310697, *15 (D.N.J. Jan. 28, 2011) (noting that that negligence is normally sufficient to warrant an adverse inference instruction); *Essenter v. Cumberland Farms, Inc.*, No. 1:09-CV-0539 (LEK/DRH), 2011 WL 124505, *4 (N.D.N.Y. Jan. 14, 2011) (granting adverse inference instruction based on the spoliating party's ordinary negligence), *with Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F. Supp. 2d 598, 614 (S.D. Tex. 2010) (stating that several Federal circuits appear to require bad faith for the imposition of an adverse inference instruction).

[19] Indeed, resolving these inconsistences was at the forefront of the Committee's goals, as the Committee explained that under the previous "limited rule . . . Federal circuits have established significantly different standards for imposing sanctions or curative measures on parties who fail to preserve electronically stored information. These developments have caused litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough." *See* Pending Rule Amendments, http://www.uscourts.gov/rules-policies/pending-rules-amendments.

To realize the Committee's "goal of establishing greater uniformity in how federal courts respond to the loss of ESI," [20] the amendments change Rule 37(e) in several ways. First, Rule 37(e)(1) provides that the court, "upon finding prejudice to another party from loss of the information, may order measures *no greater than necessary to cure the prejudice*."[21] Second, Rule 37(e)(2) eliminates the split among Federal circuits as to when an adverse inference jury instruction or other severe sanctions are appropriate when ESI has been lost. Specifically, the rule now provides that adverse inference instructions should be provided only after the court finds that a party "acted with the intent to deprive another party of the information's use in the litigation."[22] Given the need to show intent to deprive the other party of relevant material, negligence and gross negligence may no longer be a basis for imposing an adverse inference instruction.[23] Third, the Committee explained that the revised Rule 37(e) "forecloses reliance on inherent authority or state law to determine when certain measures should be used" to address the loss of ESI.[24]

III. The Impact of the Amendments to Rule 26(b) and 37(e)

A. Rule 26(b)(1)

Courts have already started to apply the revised Rule 26(b)(1). For example, in response to a request for discovery, a district court in the Third Circuit applied the proportionality factors in Rule 26(b)(1) and held that the plaintiff's request for discovery was "of, at most, minimal importance to the claims in this action and would impose a significant burden on defendants by re-opening discovery on a collateral issue."[25] Another district court in the Second Circuit applied Rule 26(b)(1) and denied a discovery request where the party had failed to illustrate that the requested production was proportional to the needs of the case.[26]

Although courts are already applying the proportionality factors under Rule 26(b)(1), the party that carries the burden of proof in a proportionality determination remains uncertain. In the cases cited above, the moving party failed to show that the requested discovery was proportional. However, a district court in the Ninth Circuit court overruled a defendant's objection to an allegedly broad discovery request because the defendant failed to demonstrate that the discovery was *not* proportional.[27] Therefore, at least for the time being, parties on both sides of a proportionality debate

---

[20] Judicial Conference, Committee on Rules of Practice and Procedure, Report of the Judicial Conference 15, Sept. 2014, http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2014.pdf.
[21] Memo from Hon. David G. Campbell, Chair, Advisory Committee on Federal Rules of Civil Procedure, to Hon. Jeffrey S. Sutton, Chair, Standing Committee on Rules of Practice and Procedure, at B-16 (June 14, 2013), http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2014-add.pdf. (emphasis supplied)
[22] Rule 37(e).
[23] FED. R. CIV. P. 37(e), Advisory Committee's Note (2015 amendments).
[24] *Id.*
[25] *Thomas v. Coopersmith*, No. CV 11-7578, 2016 WL 245317, at 9 (E.D. Pa. Jan. 20, 2016).
[26] *Henry v. Morgan's Hotel Grp., Inc.*, No. 15-CV-1789 (ER)(JLC), 2016 WL 303114, at 3 (S.D.N.Y. Jan. 25, 2016).
[27] *Morgan Hill Concerned Parents Ass'n v. California Dep't of Educ.*, No. 2:11-CV-3471 KJM AC, 2016 WL 304564, at *4 (E.D. Cal. Jan. 26, 2016).

should be prepared to present evidence and arguments assuming they carry the burden of establishing their position.

B. Rule 37(e)

As noted above, Rule 37(e)'s amendments may usher in greater uniformity in the level of culpability required to impose sanctions for the loss of ESI. In addition, the amendment's prohibition against a court's use of its inherent power to sanction parties when Rule 37(e) applies may help to solidify standards for sanctions.[28] Nevertheless, it remains uncertain whether lower levels of culpability, such as negligence, will be sufficient for sanctions for the destruction of ESI. For instance, under Rule 37(e)(1), a court may impose sanctions when it determines that the loss of ESI has prejudiced a party. This authority to sanction is not tied to any level of culpability, suggesting that it could apply to negligent conduct, so long as such conduct prejudiced another party. Therefore, as under the previous version of Rule 37(e), parties should consider necessary steps (e.g., implementing sufficient legal holds) to ensure that the routine operations of their information systems do not result in the loss of potentially relevant ESI.

It also remains unclear whether the safe harbor provision will now carry more weight with courts. For example, in the past, courts held that a party that does not have a retention/deletion policy cannot take advantage of the Rule 37(e) safe harbor.[29] Under the revised rule, parties without such policies may be able to harbor under Rule 37(e)'s protections, so long as the loss was not intentional and did not prejudice other parties. Further, the Rule's limitation on federal courts' inherent powers to sanction may cause courts to give greater consideration to Rule 37(e)'s safe harbor provision when assessing sanctions for destroying ESI.

That said, early indications in the case law suggest that courts are recognizing the new limitations in Rule 37(e). For example, a district court in the Ninth Circuit issued an adverse jury instruction before the Rule's amendment where plaintiff had "failed to prevent" the destruction of evidence.[30] After the Rule was amended, the court granted the plaintiff's motion to vacate the sanctions order, reasoning the revised Rule 37(e) did not permit an adverse inference instruction without evidence that the plaintiff intentionally engaged in spoliation.[31] Another district court in the Second Circuit recognized the limitations the amended Rule 37(e) imposes on the court's inherent authority, noting that although

[28] That said, some courts have already recognized that if Rule 37(e) does not apply (e.g., ESI is falsified but not destroyed), they may exercise their inherent authority to address discovery abuses. *See, e.g.*, *CAT3, LLC v. Black Lineage, Inc.*, No. 14CIV5511ATJCF, 2016 WL 154116, at 7 (S.D.N.Y. Jan. 12, 2016)(after discussing the new limiting language of the rule and the Committee Note, stating that "sanctions would be available under the court's inherent authority even if Rule 37(e) did not apply").

[29] *See, e.g.*, *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1191–92 (D. Utah 2009); *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 378 (D. Conn. 2007).

[30] *Nuvasive, Inc. v. Madsen Med., Inc.*, No. 13CV2077 BTM(RBB), 2016 WL 305096, at 2 (S.D. Cal. Jan. 26, 2016).

[31] *Id.* ("It is clear from the language of (e)(2) as well as the Committee Notes that the adverse inference instruction that the Court was going to give falls within the measures that are not permissible absent a finding of intent.").

sanctions "under a court's inherent power generally requires a finding of bad faith," Rule 37(e) provides for sanctions in situations where the party may not have acted in bad faith.[32]

Conclusion

By emphasizing proportionality and clarifying the scope of sanctions for the loss of ESI, the recent changes to Rule 26(b) and Rule 37(e) have great potential for reining in the increasingly unwieldy and costly e-discovery process. Indeed, based on the initial cases interpreting the revised Rules, the amendments appear to already be impacting litigation. That said, e-discovery practitioners would be well advised to closely monitor their implementation, as the issues discussed above still leave room for variations among the courts.

Khadijah Robinson *(krobinson@cov.com) is a litigation associate and a member of the E-Discovery Practice at Covington and Burling, LLP.* ***Alexander Hastings*** *(ahastings@cov.com) is a government contracts associate and a member of the firm's E-Discovery Practice.* ***Edward Rippey*** *(erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice.*

[32] *Granados v. Traffic Bar & Rest., Inc.*, No. 13CIV0500TPGJCF, 2015 WL 9582430, at 5 (S.D.N.Y. Dec. 30, 2015).

A Hidden Insider Threat: Exposing Visual Hackers

By Mari J. Frank

When we think of hackers breaching systems and stealing information from our law firms or our clients' businesses, we don't usually suspect trusted employees as the guilty parties.

But insider threats are in fact a very real and growing challenge. Security services provider SANS Institute surveyed nearly 800 IT and security professionals across multiple industries and found that 74 percent of respondents were concerned about negligent or malicious employees who might be insider threats, while 34 percent said they have experienced an insider incident or attack.[1]

Unscrupulous insiders employ alternate approaches to traditional hacking methods to gain access to networks and sensitive information. And it's this craftiness that makes them such a threat to our firms and our clients' organizations. Businesses and law firms are often so focused on technology vulnerabilities that they easily overlook risks from the human factor. Indeed, a Crowd Research Partners survey of more than 500 cybersecurity professionals found that 62 percent of respondents said insider attacks are more difficult to detect and prevent than external cyberattacks.[2]

One potential method of attack is visual hacking, which is defined as obtaining or capturing sensitive information for unauthorized use. An innocent employee may unconsciously display sensitive data which is then captured and used by an outside thief. Other unintentional insider threats occur when a trusting staff member is duped by a social engineer to divulge confidential information.

Worse yet is the intentional betrayal of a long time loyal staff member who turns rogue and uses visual hacking to acquire information they can sell to an outsider for money or revenge. Examples of visual hacking include taking photos of sensitive documents left on a printer or confidential information displayed on a screen, or simply writing down log-in information that is taped to a computer monitor. A visual hacker could be anyone within an organization's walls, including employees, contractors, service vendors, such as cleaning and maintenance crews, and even clients and other visitors.

From hacking systems to hacking people

With sophisticated system controls in place at most organizations, security hackers are finding it is easier to hack through fallible humans than complicated and well-armed systems.

---

[1] https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892

[2] http://www.businesswire.com/news/home/20150618005371/en/Report-62-Cybersecurity-Professionals-Insider-Threats-Growing#.VhaipJMlQXE

That was certainly the case when Ponemon Institute, a privacy and security research firm, conducted the Visual Hacking Experiment, which was jointly sponsored by 3M Company and the Visual Privacy Advisory Council. In the study, white-hat hackers posing as temporary or part-time workers were sent into the offices of eight U.S.-based, participating companies and were able to visually hack sensitive and confidential information from exposed documents and computer screens. They were able to visually hack information such as employee access and login credentials, accounting information and customer information in 88 percent of attempts and were not stopped in 70 percent of incidents.[3]

Unintentional Insider Threat

Careless or untrained employees or contractors can be especially easy prey for visual hackers. Such workers may be well-meaning, but they can be careless, thoughtless, or simply unaware of what to do when it comes to protecting an organization's sensitive or confidential information.

Often without considering potential consequences, employees, vendors, contractors and even board members will display confidential information in full view of others on electronic screens and printed hard copies. They may provide an easy opening for anyone to view such information when they step away from their desks. They may also share passwords, disregard security procedures or become duped by the scams or charm and persuasiveness of experienced social engineers.

Unfortunately, these behaviors are increasingly prevalent, and the liability for carelessness falls on the employer when it lacks effective policies, procedures and training regarding visual privacy best practices. Even with policies and training in place if there is a lack of enforcement, or if there are no consequences for those who fail to follow the policies, the security and privacy vulnerabilities will persist.

Intentional Insider Threat

Worse than a careless insider is a resentful, greedy or angry insider who can easily become a malevolent threat. Malicious insiders can include current or former employees, contractors, temporary staff, or anyone else who has or had authorized access to an organization's network, computer systems electronic data, or virtual or physical security features. They may be motivated by factors such as financial gain, business advantage, resentment, revenge or even ideological reasons. Using their inside knowledge of the organization and its vulnerabilities, they use savviness to prey on employees or exploit visual privacy vulnerabilities.

[3] http://news.3m.com/press-release/product-and-brand/new-study-exposes-visual-hacking-under-addressed-corporate-risk

Assess and Adapt

The best place to begin your efforts for clamping down on visual privacy threats in our firms and in our clients' organizations is to perform a visual privacy audit. This will help you assess your key-risk areas and evaluate existing security measures that are in place.

Some questions to consider when conducting a visual privacy audit include:

- Does your organization have a visual privacy policy?
- Are shredders located near copiers, printers and desks where confidential documents are regularly handled?
- Is information erased from white boards following meetings?
- Are computer screens angled away from high-traffic areas and windows, and fitted with privacy filters?
- Do employees keep log-in and password information posted at their workstations or elsewhere?
- Is there limited access confined to only those with a need to know?
- Are employees leaving computer screens on or documents out in the open when not at their desks?
- Do cabinets have a locking device for all sensitive hard copies?
- Does the organization use encryption for sensitive documents in transit or at rest?
- Do employees know to be mindful of who is on the premises and what they are accessing, photographing or viewing?
- Are there reporting mechanisms for suspicious activities?

In addition to identifying areas where visual privacy security falls short, a privacy audit can help you make changes or additions needed to your firms' policies and training.

Policies should outline the do's and don'ts of information viewing and use for employees and contractors both in the workplace and when working remotely. Performance evaluations should include adherence to privacy and security policies. Employee agreements should contain specific language about each employee's responsibility to safeguard sensitive and confidential information, both in the workplace and when working remotely.

When employees leave, the exit interview should include a thorough review and audit of the employee's paper and electronic documents, and IT should ensure employees are not able to access the organization's network after they leave the company.

Visual privacy, visual hacking and insider threat awareness must start at the top of your firm and your clients' C-suite level. It should be made an integral part of the security training, and reinforced through refresher training and employee communications.

Best Practices for Every Organization

The specific measures you take to defend against visual hacking from insider threats will be unique to firm or your clients' organization or industry. For example, health care organizations are mandated under HIPAA to use administrative, physical, and technical safeguards to ensure the privacy and security of PHI in all forms, including paper and electronic form.[4] But attorneys have a very high duty to also protect confidentiality of their cases. All organizations have the duty to protect customer and employee information, the organization's intellectual property, confidences, and privacy interests. There are some standard best practices that apply to nearly every organization.

- Implement a "clean desk" policy requiring employees to turn off device screens and remove all papers from their desks before leaving each night.
- Require applications to mask high-risk data to onlookers using strategies from most secure to least secure.
- Make shredders standard issue to all on-site units, especially by copiers, printers, faxes and a prerequisite for all who qualify to telework or qualify to use secure remote network access to corporate information assets.
- Require privacy filters on all computers and electronic device both in the office and while working remotely. Sensitive data is extremely vulnerable when staff is traveling and accessing internal networks and confidential documents. Privacy filters blacken out the angled view of onlookers while providing an undisturbed viewing experience for the user, and can be fitted to the screens of desktop monitors, laptops and mobile devices.

A Role for All Law Firms

The growing problem of insider threats shouldn't instill fear and suspicion in your staff, however we must all be aware and conscious of the threats and be proactive in preventing such hacking. The

[4] http://www.ecfr.gov/cgi-bin/text-idx?SID=cb9bd76e377bb306ee49069485dda775&node=45:1.0.1.3.78&rgn=div5#se45.1.164_1530

threat is real and all of us play an important role in helping protect our firm's sensitive data – and that of their clients and their organizations – against this increasingly prevalent problem.

Mari Frank *is a Certified Information Privacy Professional, an advisor to the State Bar of California r Law Practice Management and Technology Section, and a member of the 3 M Visual Privacy Advisory Council. She is also the host of the radio show Privacy Piracy on KUCI 88.9 FM in Irvine.*

Editor's Message

With this issue, we are well into the seventh year of publishing the *Information Law Journal* each quarter and are continuing to welcome authors and readers from similarly-focused committees across the ABA, including members from the International Law Section. This issue again presents articles from lawyers and technologists focusing on various aspects of leading-edge domestic and international practice in information law.

The first article was written by Francesca Giannoni-Crystal and Prof. Allyson Haynes Stuart, addressing how privacy and data protection is impacted by the Internet of Things. The second article is from Jason Edgecombe of Baker Donelson and Frederick Scholl of Monarch Information Networks, covering the Cybersecurity Information Sharing Act. The third article is by first time contributor Ashley L. Thomas of Hall Render, with an in-depth look at biometrics and privacy. The fourth article is written by Kate Colleary in Ireland, covering the General Data Protection Regulations' impact on business. The fifth article is from the team at Covington & Burling LLP led by partner Edward Rippey, discussing recent changes to the discovery rules under the FRCP. The sixth article is from frequent contributor Mari Frank, describing certain insider security threats for law firms. Thank you to all of the authors.

Our next issue (Summer 2016) is scheduled to be published by early June 2016. I continue to ask that all readers of the *Information Law Journal* to share their experience and knowledge with their fellow professionals by writing an article for this periodical. Every qualified submission within the scope of the periodical and meeting the requirements explained in the **Author Guidelines** will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue following the Summer issue (Autumn 2016) will be published in September 2016. As always, until then… and enjoy your springtime.