Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

THE WSGR DATA ADVISOR

SEPTEMBER 2015

Welcome

In this issue of The WSGR Data Advisor, we examine the FCC's recent TCPA declaratory ruling and order addressing issues regarding calling and texting consumers, and discuss the new privacy, data security, and transparency measures of the agency's Open Internet rules which went into effect earlier this summer. We also explore new guidance from the U.S. Department of Justice for companies responding to cyber incidents, address Delaware's new online privacy law, discuss a recent closing letter from the FTC confirming the importance of implementing strong controls on employee access to company data, and we detail a newly updated guide to protecting electronic health data from the Department of Health and Human Services.

Moving to the European Union, we examine data anonymization and pseudonymization techniques, which have been a heavily debated topic in the ongoing reform of data protection law, and we discuss what could be a significant and major first step toward creating technical standards that take privacy legal requirements into account. Finally, we detail a recent opinion that clarifies EU data protection rules in the context of civil drones.

We also hope that you can join us on September 16 in Palo Alto for The Future of Privacy in a Connected World: A Cross-Border Conversation, a discussion with European Data Protection Supervisor Giovanni Buttarelli, FTC Commissioner Julie Brill, and Special Assistant to the President David Edelman. Our panel of experts will share their thoughts on the critical privacy issues currently subject to debate in the U.S. and the EU.

As always, you can continue to email us at PrivacyAlerts@wsgr.com if there are any topics you would like to see us cover in future issues.

Lydia Parnes
Partner, Washington, D.C.
lparnes@wsgr.com

Michael Rubin
Partner, San Francisco
mrubin@wsgr.com

FCC Issues Omnibus TCPA Declaratory Ruling and Order Addressing Numerous Issues Regarding Calling and Texting Consumers

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

On July 10, 2015, the Federal Communications Commission (FCC) released its long-anticipated Declaratory Ruling and Order[1] addressing twenty-one petitions and requests seeking clarification of, and relief from, various provisions of the Telephone Consumer Protection Act (TCPA) and the FCC's implementing regulations.[2] The order provides some much-needed clarity in certain areas, but commentators have generally concluded that the order has broadened the reach of the TCPA and inserted uncertainty in other areas, making calling or texting consumers an increasingly risky business practice.

Congress enacted the TCPA in 1991 to regulate certain communications that consumers deemed an annoyance and an invasion of privacy. Among other things, the TCPA imposes requirements for telemarketing and artificial or prerecordedvoice calls to residential landline numbers, and all calls to wireless numbers and certain categories of business numbers made using an "automatic telephone dialing system" or an artificial or prerecorded voice. To encourage private enforcement, the TCPA provides for a private right of action to recover up to $1,500 per call that violates

[1] *In re* Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991, FCC 15-72 (June 18, 2015) (hereinafter "FCC order").
[2] 47 U.S.C. § 227. The FCC's TCPA rules are available at 47 C.F.R. § 64.1200 *et seq.*

In This Issue

FCC Issues Omnibus TCPA Declaratory Ruling . . . *(continued from page 1)*

the statute. Putative class actions alleging TCPA violations have increased significantly in recent years, with one source estimating that 2,336 such actions were filed in 2014 alone.[3] Therefore, businesses making calls or sending text messages to consumers are encouraged to review the FCC order and to assess its impact on their operations.

The Order

The FCC order addresses the following questions, among others:

- What equipment qualifies as an "automatic telephone dialing system" subject to the TCPA's prohibitions?
- Who is liable for TCPA violations when text messages are facilitated using apps and platforms?
- May consumers revoke consent previously given to be called/texted, and if so, how?
- Are callers liable for calls to reassigned wireless numbers when they had consent from the prior user of the number and had no knowledge of the reassignment?
- Do mobile marketers who had obtained written consent for mobile marketing campaigns prior to the effective date of the FCC's "express written consent" regulation need to re-obtain written consent?
- Do on-demand text messages sent in direct response to a consumer's request violate the TCPA if no additional consent has been provided?
- Is there an exemption from consent requirements for certain free-to-recipient calls?
- May carriers offer Do-Not-Disturb technology to customers?

Definition of "Automatic Telephone Dialing System"

The TCPA defines "automatic telephone dialing system" (which the FCC refers to as an "auto-dialer") as "equipment which has the capacity—(A) to store or produce telephone numbers to be called, using a random or sequential number generator; and (B) to dial such numbers."[4] This definition has been heavily litigated in class actions, with courts divided over: (1) a strict construction of the statutory definition (i.e., equipment needs a present capacity to generate and dial random or sequential telephone numbers to be an "auto-dialer"); and (2) a more expansive definition based on the FCC's commentary in prior rulings (i.e., an "auto-dialer" includes any system that can dial stored lists of numbers without human intervention).

In the order, the FCC denied multiple requests to clarify that the plain language of the statutory definition controls and that the FCC has not broadened that definition. Instead, in an ambiguous and confusing discussion, the FCC both relied on Congress's statutory definition and said that it would continue to apply a "without human intervention" test, using a case-by-case determination.[5] However, the order also went on to say that the term "capacity" as used in the definition does not mean "present ability," but rather "potential ability" —i.e., equipment that can generate and dial random or sequential telephone numbers with modification, reconfiguration, or addition of new software.[6] Responding to criticism from two strongly worded dissents, the majority stated that a theoretical possibility that equipment can be modified to generate and dial random or sequential numbers is not enough to make it an auto-dialer.[7] It gave examples of dialing equipment that are not auto-dialers: a handset with a speed dial function and rotary phones.[8] However, the FCC refused to define the precise boundaries of the term "capacity," leaving significant uncertainty for businesses engaged in calling or texting consumers. Several businesses have already appealed this ruling.

Texting Apps and Platforms

Numerous apps provide functionality for users to invite friends via text, or otherwise to send text messages. Businesses also use third-party texting platforms to send text messages to consumers as part of mobile marketing campaigns, for informational alerts, and for other purposes. As part of the order, the FCC resolved three petitions by app providers seeking rulings that their users initiate the texts sent through the apps, and therefore the providers have no liability under the TCPA. In resolving these petitions, the order clarifies that whether the provider is deemed an initiator of the texts (and therefore subject to TCPA requirements) depends upon the totality of the circumstances and, in particular, the provider's level of involvement in the sending of the texts.[9]

In two of the three scenarios presented in the petitions, the app users: (1) choose whether to send the messages and when; (2) choose the message recipients; and (3) control the bulk of the message content. The FCC concluded that given these circumstances, the app users initiate the messages.[10] Even where the app provider supplied the content, which promoted the app and could be considered advertising, the FCC concluded that this minimal involvement was not enough to make the app provider responsible for the messages.[11]

---

[3] "Debt Collection Litigation & CFPB Complaint Statistics, December 2014 & Year in Review," WebRecon LLC, January 22, 2015, http://dev.webrecon.com/debt-collection-litigation-cfpb-complaint-statistics-december-2014-and-year-in-review/.
[4] 47 U.S.C. § 227 (a)(1).
[5] FCC Order, *supra* note 1, at para. 17.
[6] *Id.* at para. 19.
[7] *Id.* at para. 18.
[8] *Id.*
[9] *Id.*at para. 30.
[10] *Id.* at paras. 32, 37.
[11] *Id.* at para. 37.

Continued on page 3...

FCC Issues Omnibus TCPA Declaratory Ruling . . . *(continued from page 2)*

In a third scenario, where the app provider was alleged to have automatically sent invitation text messages to all of its users' cell phone contacts with little or no involvement of the users, the FCC concluded that the app provider was the initiator.[12] This is a beneficial ruling for app and texting platform providers, as they can design their services to conform to the ruling so that they can facilitate others' sending text messages without opening themselves up to TCPA liability.

Revoking Consent to Calls

The FCC order makes clear that consumers may revoke consent. It also concludes that a consumer may revoke consent through any reasonable means that clearly expresses a desire not to receive further calls or messages.[13] Reasonable means may include oral or written opt-out requests.[14] The order rejects the notion that businesses can require revocation only in writing or by other limited means.[15] Multiple appeals have been filed arguing that this ruling, among other things, imposes an undue compliance burden on businesses.

Calling Wireless Numbers No Longer Associated with the Person Who Provided Consent

The order concludes that for consent to be valid under the TCPA, it must be obtained from the current subscriber to the number, or a non-subscriber who is a customary user of the phone (e.g., a family member on a family plan).[16] According to the FCC, consent to call a number obtained from the intended recipient of the call when the number has been reassigned to someone else is insufficient, even though the calling party had no knowledge of the reassignment.[17]

Numerous parties had petitioned the FCC to clarify the meaning of the phrase "called party" within the section of the TCPA that excludes from the law's coverage any calls made "with the prior express consent of the called party." Those petitions explained that there is no database of reassigned numbers or other means for callers to know in all instances that a number has been reassigned, which has led to significant TCPA class action litigation. Although the FCC recognized this reality, it rejected the plea to fix this problem.

> The FCC order makes clear that consumers may revoke consent

In light of the significant impact of this ruling —which plainly stands to chill a significant amount of protected speech and likely violates the Due Process rights of callers—the FCC adopted a "one free call" exception. Under this exception, a caller may initiate one call to a call recipient after a number reassignment without incurring TCPA liability.[18] However, the exception has limited value since it is limited to one call even if the called party does not answer or respond, and even if the caller does not obtain knowledge of the number reassignment through that call.[19] Therefore, this exception may not be helpful to callers in most cases.

To take advantage of this exception, the caller must be able to show that it made the one-time call without knowledge of the reassignment and with a reasonable basis to believe that it has a valid consent to make the call.[20] If the one-time call does not provide actual knowledge of whether reassignment occurred, the caller is deemed to have constructive knowledge that the number was reassigned—a position that these writers believe makes no sense. The FCC suggests several alternative options for determining whether a number has been reassigned, such as by signing up for number reassignment databases (which the FCC acknowledge are incomplete) and regular email communications with consumers to verify contact information.[21] This ruling also is the subject of several appeals.

Updating Prior Express Written Consent Obtained Under Old Rules

Effective October 16, 2013, the FCC made material changes to its TCPA regulations affecting the consumer consent requirements applicable to certain calls and messages.[22] Under the TCPA, "prior express consent" is required for calls and texts to wireless numbers and certain other types of calls. In the amended regulations, the FCC made a distinction between calls/texts that are purely informational and calls/texts that introduce an advertisement or that amount to telemarketing. For marketing/advertising calls or messages to wireless numbers using an "automatic telephone dialing system"

[12] *Id.* at para. 34.
[13] *Id.* at para. 63.
[14] *Id.* at para. 64.
[15] *Id.* at para. 47.
[16] *Id.* at para. 73.
[17] *Id.* at para. 83.
[18] *Id.* at para. 72.
[19] *Id.*
[20] *Id.*
[21] *Id.* at para. 86.
[22] *See In re Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991,* CG Docket No. 02-278 Report and Order, FCC 12-21, ¶ 4 (February 15, 2012).

Continued on page 4...

FCC Issues Omnibus TCPA Declaratory Ruling . . . *(continued from page 3)*

or artificial or prerecorded voice message (as well as artificial or prerecorded voice marketing/advertising calls to residential lines and certain categories of calls to business lines), prior express *written* consent, obtained in the manner specified in the FCC's regulations, is required by the FCC.[23] Prior to the effective date of the amended regulation, consent could be provided orally or in writing for these types of calls.

Multiple mobile marketing organizations petitioned the FCC to clarify that when their members had obtained written consent (such as through a double opt-in) for ongoing campaigns prior to October 16, 2013, they were not required to re-opt in those users to comply with the new written consent requirements. The FCC order rejected those requests and stated that re-opt in is required to ensure that the disclosures required by the updated consent regulation were provided.[24] However, the FCC granted a limited waiver of the updated consent regulation until October 7, 2015, so that members of the petitioning organizations can come into compliance.

On-Demand Text Messages

The order concludes that one-time text messages sent immediately after a consumer's request for the message does not violate the TCPA because the sender is merely fulfilling the consumer's request even if the text otherwise would be deemed telemarketing.[25] The one-time text message must: (1) have been requested by the consumer; (2) be sent immediately in response to the request; and (3) contain only the information requested by the consumer and no other marketing or advertising language.[26] A one-time text message may be commercial in nature, such as sending coupon codes in response to a consumer inquiry. This is a very helpful ruling for companies that engage in mobile marketing.

Exemptions for Certain Free Calls

The order permits certain free-to-end-user urgent financial or healthcare-related calls and text messages without prior express consent from consumers.[27] First, when certain conditions are met, the FCC exempted from the TCPA's prior-express-consent requirement any messages from financial institutions intended to: (1) prevent fraudulent transactions or identity theft; (2) alert consumers to data breaches at retailers and other businesses that pose a security threat to the customers' financial account information; (3) instruct customers on measures to take to prevent identity theft following a data breach; and (4) communicate information regarding money transfers.[28] Second, the FCC exempted from the TCPA's prior-express-consent requirement any messages from entities regulated by HIPAA that meet certain conditions and "for which there is exigency and that have a healthcare treatment purposes, specifically: appointment and exam confirmations and reminders, wellness checkups, hospital pre-registration instructions, pre-operative instructions, lab results, post-discharge follow-up intended to prevent readmission, prescription notifications, and home healthcare instructions."[29]

Call-Blocking/Do-Not-Disturb Technology

In the order, the FCC affirmed that carriers and VoIP providers may offer and implement call-blocking technology to help consumers block calls or categories of calls that come from consumer-selected sources.[30] However, the FCC cautioned carriers and VoIP providers to avoid blocking autodialed or prerecorded calls from public safety, emergency, city or school, or law enforcement entities.[31] The FCC was concerned that blocking such calls may negatively affect local and state emergency alerting and communications efforts.[32] The FCC stated that certain disclosures may be offered to consumers, such as notice that the blocking technology may inadvertently block wanted calls.[33] The FCC also suggested that carriers and VoIP providers permit customers to review a list of blocked calls to report and correct blocking errors.[34]

The FCC order covers a wide variety of TCPA-related requirements and shows how complicated and nuanced compliance may be. The compliance burden is even greater when taking into account the many state mini-TCPA and telemarketing statutes. Businesses calling consumers may wish to review and update their policies and procedures to account for FCC orders, as well as other applicable federal and state laws.

---

[23] 47 C.F.R. §§ 64.1200 (a)(2), (a)(3).
[24] *Id.* at para. 100.
[25] *Id.* at paras. 103, 104.
[26] *Id.* at para. 106.
[27] *Id.* at para. 125.
[28] *Id.* at paras.129-131.
[29] *Id.* at para. 146.
[30] *Id.* at para. 152.
[31] *Id.*
[32] *Id.*
[33] *Id.* at para. 160.
[34] *Id.* at para. 161.

FCC Open Internet Rules Contain Important New Privacy, Data Security, and Transparency Measures

Victoria Jeffries
Associate, Washington, D.C.
vjeffries@wsgr.com

Ted Serra
Associate, Washington, D.C.
tserra@wsgr.com

Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

The Federal Communication Commission's (FCC's) newly promulgated Open Internet rules (2015 rules)—also known as the net neutrality rules—went into effect on June 12, 2015.[1] The new rules apply specifically to broadband Internet access service providers, and not to Internet content, application, and device providers (edge providers). Nonetheless, by design, the rules will have a potentially far-reaching impact on edge providers' and consumers' rights and the avenues for redress in the face of harm inflicted by broadband providers. To date, the FCC has yet to receive any formal complaints from companies, though those may well be in the offing, according to some media reports and public statements.[2]

As anticipated, telecommunications and broadband providers[3] filed challenges to the 2015 rules at the U.S. Court of Appeals for the D.C. Circuit in July 2015. Oral arguments are scheduled for December 4, 2015. Media coverage—and to a large extent the legal challenges brought against the 2015 rules—have focused on the FCC's decisions to reclassify fixed and mobile broadband providers as common carriers and to prohibit Internet traffic blocking, throttling, and prioritization. Other aspects of the new rules, however, also have important implications for the Internet economy, as the new rules address deceptive and unfair practices by broadband providers, consumer data security and privacy, and the transparency of information available to consumers and edge providers.

The FCC concluded in 2010, and again in 2015,[4] that Internet openness fosters a virtuous cycle in which Internet-based application, service, and device innovation increases broadband use, which leads to the expansion and improvement of broadband infrastructure. That, in turn, fosters further application, service, and device innovation.[5] The FCC found that privacy protections are a fundamental aspect of the virtuous cycle because privacy-related concerns might otherwise decrease Internet usage, thereby threatening to disrupt the cycle.[6]

FCC to Take On Deceptive and Unfair Practices

The 2015 rules prohibit broadband providers from "unreasonably" discriminating against Internet content, applications, or devices, relying on a catch-all "no unreasonable interference/disadvantage" standard.[7] While a discriminatory practice that is reasonable network management does not violate the rules,[8] the FCC will conduct a case-by-case analysis to determine whether a practice unreasonably interferes with or disadvantages consumers' access to edge providers. Among other factors, the FCC will consider whether a broadband provider employs "any deceptive or unfair practices," including those that "fail to protect the confidentiality of end users' proprietary information."[9] Importantly, a given practice may violate the new standard only when it *unreasonably interferes* with consumers' ability to use or access lawful Internet content.

This seemingly narrow category of activities prohibited by the 2015 rules contrasts with the Federal Trade Commission's (FTC's) broader consumer protection standard. The FTC has a long track record of using its authority under Section 5 of the FTC Act to protect consumers from "unfair or deceptive acts or practices," including (and increasingly) those related to data privacy and security.[10] The FTC's deception standard,

---

[1] "Protecting and Promoting the Open Internet," Final Rule, 80 Fed. Reg. at 19737 (April 13, 2015); 47 CFR pts. 1, 8, 20.

[2] *See e.g.*, David Schaeffer, Cogent Communications, Remarks at Q2 2015 Earnings Call (August 6, 2015) (describing how negotiations with some ISPs have stalled and that Cogent is preparing to seek enforcement action and/or litigation); Margaret Harding, "Industry Moves Closer to First FCC Net Neutrality Complaint," *Law360*, August 11, 2015, http://www.law360.com/articles/689915/industry-moves-closer-to-1st-fcc-net-neutrality-complaint.

[3] Petitioners include: Alamo Broadband, the American Cable Association (ACA), AT&T, CenturyLink, the Cellular Telephone Industries Association (CTIA), the National Cable & Telecommunications Association (NCTA), USTelecom, and the Wireless Internet Service Providers Association (WISPA).

[4] The previous Open Internet rules put forth by the FCC in 2010 were largely struck down by the D.C. Circuit in *Verizon v. FCC. In re Preserving the Open Internet*, 25 F.C.C.R. 17905 (2010); 740 F.3d 623 (D.C. Cir. 2014). The D.C. Circuit's decision left the 2010 transparency rule undisturbed; the 2015 rules not only adopt the 2010 transparency rules, but also expand and add privacy measures.

[5] "Protecting and Promoting the Open Internet," 80 Fed. Reg. at 19739.

[6] *Id.* at 19814-15.

[7] *Id.* at 19756.

[8] *Id.* "A network management practice is a practice that has a primarily technical network management justification, but does not include other business practices. A network management practice is reasonable if it is primarily used for and tailored to achieving a legitimate network management purpose, taking into account the particular network architecture and technology of the broadband Internet access service." *Id.* at 19741.

[9] *Id.* at 19757.

[10] 15 U.S.C. § 45 (a)(1). *E.g.*, Decision and Order, *In re Snapchat, Inc.*, FTC No. 1323078 (December 23, 2014) (alleged violations of Section 5 when deceptively marketing mobile application that could send temporary messages that would disappear after a certain time period); Decision and Order, *In re Aaron's Inc.*, FTC No. 1223264 (March 10, 2014) (alleged violations of Section 5 when using installed software on computers rented to consumers to log keystrokes, take screenshots, and employ webcams without consumers' knowledge in a way that was unfair to consumers); Decision and Order, *In re HTC America, Inc.*, FTC No. 1223049 (June 25, 2013) (alleged violations of Section 5 when failing to employ reasonable security on mobile devices).

Continued on page 6...

FCC Open Internet Rules . . . *(continued from page 5)*

for instance, does not require actual injury, but rather applies to practices that are *likely* to cause consumer harm. The FTC's unfairness standard applies to any practice that causes actual and substantial harm, not just practices that could interfere with consumers' ability to use or access lawful Internet content.[11] Prior to the 2015 rules, the FTC may have had jurisdiction over broadband providers when they provided broadband services and not common carrier services.[12] Now that the 2015 rules have reclassified broadband Internet access services as a "common carrier" service under Title II of the Communications Act, at least one provider of broadband Internet access services, AT&T, has challenged the FTC's jurisdiction over AT&T's practices. AT&T has argued that the FTC Act's "common carrier" exemption from the FTC's jurisdiction applies to entities based on their status as a common carrier, not just based on common carrier activities. The FTC asserted, and a district court agreed, that it properly has jurisdiction over AT&T's non-common carrier activities.[13] In early August 2015, the U.S. Court of Appeals for the Ninth Circuit agreed to hear AT&T's appeal of that determination and will review briefs later this fall.[14]

Data Privacy and Security Requirements

The Communications Act imposes a number of obligations on common carriers, including a duty to protect the confidentiality of customers' proprietary information.[15] The FCC's 2015 rules newly apply the Communication Act's provisions related to data privacy—previously applicable to voice telecommunications services—to broadband providers.[16] Now, except as expressly authorized by customers or otherwise required by law, a broadband provider that possesses individually identifiable customer proprietary network information (CPNI) will only be permitted to use or disclose CPNI for the purpose of providing the broadband Internet service.[17] As applied to voice telecommunications services, this privacy restriction has not applied to aggregate customer information.[18] The CPNI definitions applicable to broadband Internet access services, though, have not yet been resolved. Chairman Wheeler has stated that the FCC will likely launch a rulemaking on broadband definitions for CPNI this coming fall.[19] The broadband equivalent of the FCC's CPNI rules could encompass a broad swath of information such as, for example, data generated when a consumer visits a website through a web browser or mobile application—increasingly valuable information for advertisers and content providers.

Enhanced Transparency Rule

The 2015 rules expand the scope and detail of the FCC's previously issued transparency rule, which survived the D.C. Circuit's *Verizon* decision. The enhanced transparency rule is intended to ensure that consumers and edge providers will have the information they need to evaluate different broadband providers' service offerings—including technical performance characteristics. Under the new transparency rule, broadband providers now *must* disclose more detailed information about network practices, performance characteristics, and commercial terms.[20] The 2010 Open Internet rules merely suggested, in some instances, the kinds of detailed disclosures that might be appropriate. Required disclosures include terms related to pricing, privacy policies, data caps or allowances, and other fees.[21] Disclosures in privacy policies should include "whether network management practices entail inspection of network traffic, and whether traffic information is stored, provided to

---

[11] 15 U.S.C. § 45(n). Under the FTC's unfairness standard, substantial and actual harm is weighed against any "countervailing benefits to consumers or to competition." *Id.*

[12] Order Denying Defendant's Motion to Dismiss, *Fed. Trade Comm'n v. AT&T Mobility LLC*, No. C-14-4785 EMC (N.D. Cal. March 31, 2015) (holding that the FTC Act's common carrier exception applies only when: (1) the entity has the legal status of a common carrier, and (2) the entity is performing common carrier activities).

[13] Order Denying Defendant's Motion to Dismiss, *FTC v. AT&T Mobility LLC*, No. 14-C-4785 (N.D. Cal. March 31, 2015).

[14] Order, *FTC v. AT&T Mobility LLC*, No. 15-16585 (9th Cir. August 10, 2015).

[15] 47 U.S.C. § 222. Customers' proprietary information includes information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service and information contained in customers' bills. § 222 (h)(1).

[16] "Protecting and Promoting the Open Internet," 80 Fed. Reg. at 19814. The FCC exercised its so-called forbearance prerogative by temporarily refraining from imposing on broadband providers many of the Communications Act's statutory provisions and associated rules currently applicable to telecommunications services. Some of the provisions that the FCC forbore from applying to broadband providers include the requirement to unbundle networks, the requirement to provide service in some circumstances, and rate regulation.

[17] § 222 (c)(1). The FCC had previously issued rules implementing the statutory privacy provision, but those rules are specific to voice calls, and the FCC decided not to apply those implementing rules to broadband providers. "Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information," Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 (2007); "Protecting and Promoting the Open Internet," 80 Fed. Reg. at 19815. The FCC stated that it will develop new implementing rules applicable to broadband providers, and suggested that customers' web browsing history was sensitive information that would be protected under such rules. "Protecting and Promoting the Open Internet," 80 Fed. Reg. at 19815.

[18] "The term 'aggregate customer information' means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed." § 222 (h)(2).

[19] Tom Wheeler, FCC Chairman, "Maximizing the Benefits of Broadband," Remarks at the Brookings Institution (June 26, 2015) (transcript and recording, http://www.brookings.edu/events/2015/06/26-maximizing-benefits-broadband-wheeler); Brian Fung, "The Messy Battle to Protect Your Data from Your Own Internet Provider," *The Washington Post*, August 20, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/08/20/the-messy-battle-to-protect-your-data-from-your-own-internet-provider/.

[20] Specifically, the transparency rule requires that broadband Internet service providers disclose: "(1) network practices, including congestion management, application-specific behavior, device attachment rules, and security measures; (2) performance characteristics, including a general description of system performance and the effects of specialized services, if any, on available capacity; and (3) commercial terms, including pricing, privacy policies, and redress options." "Preserving the Open Internet, Broadband Industry Practices," Report and Order, 25 FCC Rcd 17905, 17938-39, para. 54 (2010).

[21] "Protecting and Promoting the Open Internet," 80 Fed. Reg. at 19760.

Continued on page 7...

FCC Open Internet Rules . . . *(continued from page 6)*

third parties, or used by the carrier for non-network management purposes."[22] The FCC also clarified that broadband providers have a duty to update their mandatory disclosures in a timely manner whenever there is a material change in the terms or circumstances.[23]

Of special interest to edge providers, the enhanced transparency rule newly requires that broadband providers use packet loss as a measure of network performance.[24] The previous transparency rule already required actual network performance disclosures related to speed and latency.[25] Separately, broadband providers also now will be required to send a specific notification to consumers when a "network practice" is likely to significantly affect their use of the service.[26] Finally, the 2015 rules adopt a voluntary safe harbor for broadband providers that elect to use a consumer disclosure format the FCC will promulgate in late 2015.[27] The FCC expects that the format will be "clear and easy to read—similar to a nutrition label" so that consumers can easily compare different broadband providers.[28]

Edge Provider and Consumer Avenues for Redress

If edge providers or consumers believe that they are being harmed by a broadband provider's practices that may violate the 2015 rules, the FCC has put forth three ways that those concerns may be addressed.[29] Edge providers or consumers can formally or informally submit complaints to the FCC about the practices of broadband providers.[30] Additionally, edge providers or broadband providers that are unsure whether a practice or commercial arrangement may run afoul of the 2015 rules may seek an advisory opinion from the FCC before implementing them.[31] The FCC will not bring an enforcement action against a requesting party acting in good-faith reliance upon an advisory opinion, so long as the request was truthful and fulsome, and the resulting activity matches that proposed in the request.[32] Nevertheless, the FCC reserves the right to reconsider an issue addressed by an advisory opinion and to rescind or revoke an opinion.[33]

Under the auspices of the 2015 rules, the FCC has signaled that privacy and consumer protection is one of its key enforcement priorities. Challenges to the rules from broadband providers do not appear to have slowed or otherwise chilled the FCC's enforcement agenda.[34] In the coming year, we will begin to see the practical bounds and implications of these new consumer protection measures as they are implemented by the FCC and reviewed by courts.

[22] *Id.* at 19761.
[23] *Id.* at 19760.
[24] *Id.* at 19761.
[25] *Id.*
[26] *Id.*
[27] *Id.* at 19763.
[28] *Id.*
[29] *Id.* at 19742.
[30] *Id.* at 19771.
[31] *Id.* at 19772. The requests and opinions will be publicly available and are intended to guide the Internet industry. *Id.* at 19773.
[32] *Id.* at 19773.
[33] *Id.*
[34] *See e.g.*, FCC Press Release, "TerraCom and YourTel to Pay $3.5 Million to Resolve Consumer Privacy and Lifeline Investigations," July 9, 2015, https://apps.fcc.gov/edocs_public/attachmatch/DOC-334286A1.pdf; FCC Press Release, "Enforcement Bureau Guidance: Broadband Providers Should Take Reasonable, Good Faith Steps to Protect Consumer Privacy," May 20, 2015, https://apps.fcc.gov/edocs_public/attachmatch/DA-15-603A1.pdf; FCC Press Release, "FCC Joins Asia Pacific Privacy Authorities," April 15, 2015, https://apps.fcc.gov/edocs_public/attachmatch/DOC-333037A1.pdf.

DOJ Issues Guidance for Responding to Cyber Attacks

Donald Vieira
Partner, Washington, D.C.
dvieira@wsgr.com

Joseph Molosky
Associate, Washington, D.C.
jmolosky@wsgr.com

Cyber attacks can result in significant monetary and reputational damage to a wide range of businesses. Recently, the U.S. Department of Justice (DOJ) increased its efforts to engage businesses on cybersecurity issues. Earlier this year, as part of that effort, the department published a new resource for companies victimized by a cyber attack. The guidance, "Best Practices for Victim Response and Reporting of Cyber Incidents," is targeted at smaller organizations, but it provides beneficial insights for companies of all sizes, including best practices for preparing for, responding to, and recovering from cyber incidents that are applicable to all organizations.[1]

[1] DOJ, "Best Practices for Victim Response and Reporting of Cyber Incidents" (April 2015), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf.

Continued on page 8...

DOJ Issues Guidance for Responding to Cyber Attacks . . . *(continued from page 7)*

Preparing for Cyber Attacks

As part of any company's efforts to prepare for a cyber incident, the guidance stresses the importance of conducting a risk assessment to evaluate a company's assets and to assess the policies and procedure in place to protect those assets. For example, the guide recommends identifying a company's "Crown Jewels"— mission critical data and assets—and then implementing security and risk management practices to protect these key assets. The guide also suggests implementing an actionable cyber incident response plan *before* any incidents occur, as the company may not have the time and resources available following an incident to establish a plan for responding. The DOJ also recommends establishing relationships with relevant third parties and related stakeholders, such as law enforcement officials and forensic and investigative service providers, prior to an incident. The DOJ recommends that this outreach include legal counsel, as cyber attacks can raise a multitude of unique and difficult legal issues.

The costs of ineffective response to a cyber attack can be significant

Responding to a Cyber Attack

The DOJ recommends that companies respond to incidents utilizing a four-step response process. First, immediately upon learning of an incident, the guidance recommends that a company conduct an initial assessment of the nature and scope of the cyber incident. According to the guidance, the assessment should be used to address the scale of the incident and the resources available inside the company to deal with the incident. A company should also consider additional assistance it may need from law enforcement and/or legal and forensic service providers. Importantly, the department recommends that companies document as much information as available about an incident, especially in the event that a company suspects that a criminal incident occurred.

Second, the guidance recommends that a company implement measures to minimize continuing damage from a cyber attack, in the event that the attack is ongoing when identified by the company. Mitigation may include efforts as significant as barring all external access to the company's network and systems in the event of an intrusion or monitoring the illegal activity to gather more information about the attack. The specific recommended actions for this step depend heavily on the type, complexity, and timing of the attack and the assets impacted. The guidance recommends maintaining detailed records of the actions taken (or not taken) for this step, which are also important for potential litigation and criminal investigations.

Third, the guidance recommends that a victim company collect and record information about the attack, including imaging affected computers and devices for future investigative use. This step includes maintaining logs and records about attacks, such as a description of the attack, the people, service providers, and tasks involved in addressing the attack, the data, systems, and assets affected, and any continuing activity of the attack.

The final recommendation is that a company should notify affected stakeholders, including senior management, legal counsel, IT and security personnel, and the public relations department. This recommendation includes notifying law enforcement and the Department of Homeland Security, as appropriate, to obtain assistance in addressing the cyber attack and to share details about the attack to help prevent additional incidents. Depending on the information affected by the attack, data breach notification laws and contractual requirements may require that a company notify affected consumers, vendors, service providers, clients, and/or investors. Companies should carefully consider the legal and business risks associated with these external notifications with appropriate legal counsel.

Recovering from a Cyber Attack

Finally, the DOJ provides brief guidance on recovering from a cyber attack. The guidance recommends against using any of the systems and assets compromised by the attack to communicate about an incident, including the efforts to respond to the incident. Importantly, the guide also recommends against victim companies hacking into or damaging another network or system involved in an attack as a response to an intrusion. The guidance stresses that there may be legal liability for so-called hacking-back efforts and the potential for increasing the damage to the company from the attack if the original attacker retaliates.

Implications

While the DOJ's guidance is directed at small companies, the guidance provides a model for all companies to utilize to evaluate their current data breach and incident response practices. As the guide recommends, companies, especially those with less sophisticated compliance and security programs, should take care to utilize experts whenever possible, as the legal and regulatory landscape for cyber attacks, security incidents, and data breaches is very active and constantly evolving. The recommendations for information sharing are also topics of great concern for law enforcement and government agencies, and companies should carefully consider both the risks and benefits of participating in such programs. The costs of ineffective preparation for and response to a cyber attack can be significant, and the DOJ's guide provides a strong starting point for addressing these risks.

Delaware Enacts New Online Privacy Laws

Edward Holman
Associate, Washington, D.C.
eholman@wsgr.com

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Tracy Shapiro
Of Counsel, San Francisco
tshapiro@wsgr.com

Beginning January 1, 2016, the recently-enacted "Delaware Online Privacy and Protection Act"[1] (DOPPA) will take effect and will impact all companies with online services used by Delaware residents. DOPPA consists of three separate online privacy laws: (1) a law prohibiting certain types of online marketing or advertising to minors;[2] (2) a law requiring commercial websites and online services to post privacy policies;[3] and (3) a law restricting government access to user records kept by online book service providers.[4] The laws are substantively similar to online privacy laws already in effect in other states, and are particularly similar to laws in effect in California. The Consumer Protection Unit of the Delaware Department of Justice can enforce DOPPA's three laws under the same provisions that it enforces other state consumer protection laws.[5] DOPPA does not create a private right of action for any of the three laws.[6]

The Delaware Online Privacy and Protection Act

DOPPA's prohibition on certain types of online marketing or advertising to minors mirrors the prohibitions in California Business & Professions Code Section 22580.[7] As under California law, DOPPA prohibits operators of websites, online or cloud computing services, online applications, or mobile applications "directed to children"[8] from marketing or advertising certain specified categories of products and services that minors would not legally be able to purchase, and prevents them from "knowingly" using, disclosing, or compiling minors' personal information for such marketing or advertising, or allowing a third party to do so.[9] The prohibited products and services largely overlap with those listed in the California law. The differences include graffiti-related products and e-cigarettes,[10] which are only listed in the California law, and body piercing and tongue-splitting services,[11] which are only listed in the Delaware law. The Delaware law suffers from the same vagueness issues as the California law. For example, whether a site is directed to children under 18 is a much more difficult analysis than whether a site is directed to children under 13, and while the law provides an exception for the "incidental placement" of products in content that is not distributed "primarily for the purposes of marketing and advertising,"[12] those concepts leave significant room for interpretation.

Similarly, DOPPA's requirement that commercial websites and online services post privacy policies is virtually identical to the California Online Privacy Protection Act (CalOPPA),[13] including CalOPPA's "Do Not Track" disclosure requirements.[14] Both laws require an operator of a website or online service that collects personally identifiable information (broadly defined) to conspicuously post a privacy policy disclosing what categories of information the operator collects and with whom that information is shared, among other requirements. The only notable difference between the two laws is that DOPPA expressly includes "cloud computing service[s], online application[s], [and] mobile application[s]," while those categories are not specifically listed in CalOPPA (although the California Attorney General would presumably argue that CalOPPA applies to those services as types of "online services"[15]). Thus, companies complying with a broad interpretation of CalOPPA should also be in compliance with DOPPA's privacy policy requirements. As with CalOPPA, operators under DOPPA will not be in violation of the privacy policy requirements unless they fail to remediate any noncompliance issues within 30 days of being notified of those issues by the state.[16]

Finally, DOPPA's restriction on government access to user records kept by online

---

[1] Del. Code tit. 6, §§ 1201C-1206C (eff. Jan 1, 2016).
[2] *Id.* § 1204C.
[3] *Id.* § 1205C.
[4] *Id.* § 1206C.
[5] *Id.* § 1203C.
[6] Similar state laws are sometimes sought to be enforced privately as part of other state consumer protection statutes, or create a private right of action expressly. *See, e.g.*, California's Reader Privacy Act, Cal. Civ. Code § 1798.90-1798.90.05, discussed *infra*.
[7] Cal. Bus. & Prof. Code § 22580 is the first half of what is commonly known as the "Eraser" bill. Delaware's law does not contain the "eraser" provisions of Cal. Bus. & Prof. Code § 22581.
[8] The Act defines a "child" or "children" to be one or more Delaware residents under the age of 18. *Id.* § 1202C(6).
[9] *Id.* § 1203C(a).
[10] Cal. Bus. & Prof. Code § 22580(i)(5), (6), (17).
[11] Del. Code tit. 6, § 1204C(f)(11), (15).
[12] *Id.* § 1204C(h).
[13] Cal. Bus. & Prof. Code § 22575-79.
[14] *Compare id.* § 22575(b)(5), *with* Del. Code tit. 6, § 1205C(b)(5).
[15] *See* California Department of Justice, Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy 6 (2014) ("[CalOPPA] does not define 'online service,' although the Attorney General has stated that a mobile application is one type of online service."), https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.
[16] Del. Code tit. 6, § 1205C(a).

Continued on page 10...

Delaware Enacts New Online Privacy Laws . . . *(continued from page 9)*

book service providers[17] is essentially a scaled-back version of California's Reader Privacy Act.[18] Both acts consist of two key sections: (1) a section that prohibits book service providers from disclosing user information to state law enforcement or other state government entities, and from being compelled to provide user information to other individuals, except under certain defined circumstances;[19] and (2) a section imposing certain public reporting requirements on book service providers regarding the number and types of requests for user information received by the provider.[20] There are, however, some key distinctions between the two acts that make Delaware's restrictions more limited. First, Delaware's requirements only apply to online book sales or services, not brick-and-mortar book retailers that do not have an online presence, while California's requirements apply to all stores.[21] Both states' requirements only apply if the retailer's sales from books or book services exceed two percent of the retailer's gross annual sales of all consumer products.[22] Second, Delaware does not impose any civil penalties for violations of the requirements, while California allows for civil penalties up to $500 per violation and includes a private right of action.[23] Finally, Delaware imposes substantively less stringent requirements on law enforcement and government agencies seeking access to user information from book service providers. For example, Delaware's law only requires that a law enforcement entity use "any lawful method or process by which a law enforcement entity is permitted to obtain such information," while California's law requires the law enforcement entity to obtain a court order with probable cause and other strict requirements.[24]

Implications

Ultimately, DOPPA's three laws should hold few surprises for businesses already complying with California's "Eraser" bill, CalOPPA, and California's Reader Privacy Act. Businesses marketing products and services to minors will want to add Delaware's new restricted products to their list of items to block for compliance purposes. Similarly, online booksellers and book service providers will want to update their required Reader Privacy Act reports to include information relevant to Delaware.

[17] A "book service provider" under DOPPA is "any commercial entity offering a book service to the public, except that a commercial entity that sells a variety of consumer products is not a book service provider if its book service sales do not exceed 2 percent of the entity's total annual gross sales of consumer products sold in the United States." *Id.* § 1202C(5). A "book service" is "a service by which an entity, as its primary purpose, provides individuals with the ability to rent, purchase, borrow, browse, or view books electronically or via the Internet." *Id.* § 1202C(3). A "book" is "paginated or similarly organized content in digital, electronic, printed, audio, or other format, including fiction, nonfiction, academic, or other works of the type normally published in a volume or finite number of volumes, excluding serial publications such as a magazine or newspaper." *Id.* § 1202C(2).
[18] Cal. Civ. Code § 1798.90-1798.90.05.
[19] Del. Code tit. 6, § 1206C(a); Cal. Civ. Code § 1798.90(c).
[20] Del. Code tit. 6, § 1206C(e); Cal. Civ. Code § 1798.90(i)-(k).
[21] *Compare* Del. Code tit. 6, § 1202C(3), (5), *with* Cal. Civ. Code § 1798.90(b)(2).
[22] Del. Code tit. 6, § 1202C(5); Cal. Civ. Code § 1798.90(b)(2).
[23] *Compare* Del. Code tit. 6, § 1206C(d), *with* Cal. Civ. Code § 1798.90(g).
[24] *Compare* Del. Code tit. 6, § 1206C(a)(1), *with* Cal. Civ. Code § 1798.90(c)(1).

FTC Closing Letter Confirms the Importance of Implementing Employee Access Controls

Tracy Shapiro
Of Counsel, San Francisco
tshapiro@wsgr.com

Joseph Molosky
Associate, Washington, D.C.
jmolosky@wsgr.com

Companies have been pressing the Federal Trade Commission (FTC) for additional guidance on data security, and the agency recently delivered. On August 10, 2015, the FTC issued a public closing letter to Morgan Stanley Smith Barney LLC (Morgan Stanley) regarding the agency's investigation into concerns that the company "fail[ed] to secure, in a reasonable and appropriate manner, account information related to Morgan Stanley's Wealth Management clients."[1] In the context of data security investigations, closing letters—which explain why FTC staff opted to close an investigation—have the potential to offer helpful insights on what security measures the FTC considers to be reasonably designed to protect the privacy and security of personal information. Knowing what factors influenced the FTC staff's decision to close

[1] FTC, Closing Letter to Morgan Stanley Smith Barney LLC, August 10, 2015, https://www.ftc.gov/system/files/documents/closing_letters/nid/150810morganstanleycltr.pdf.

Continued on page 11...

FTC Closing Letter Confirms the Importance . . . *(continued from page 10)*

an investigation in one instance is equally instructive as knowing why the staff decided to pursue an enforcement action in another.

Morgan Stanley Data Breach

In January 2015, a Morgan Stanley employee admitted to inappropriately transferring account information for 350,000 Morgan Stanley clients from the company's network to a personal website and then to a personal device. Hackers then reportedly accessed some of this information and posted account information, including client names, account numbers, and investment details, for 1,200 clients on multiple public websites.[2] Upon learning of this data breach, the FTC initiated an investigation into Morgan Stanley's data security practices to determine whether the company engaged in unfair or deceptive acts or practices in violation of Section 5 of the FTC Act by failing to implement reasonable security measures to protect the clients' account information.

FTC Closing Letter

On August 10, 2015, the FTC sent a letter to Morgan Stanley notifying the company that it was closing its investigation because Morgan Stanley had "established and implemented comprehensive policies designed to protect against insider theft of personal information." The letter explained that Morgan Stanley had in place a policy limiting employee access to only the personal information for which they had a business need. Morgan Stanley also had processes in place to limit or prevent employees' transferring of personal information, including monitoring the size and frequency of data transfers by employees, prohibiting employee use of USB and similar devices for transferring information, and blocking employee access to certain high-risk websites and applications. During its investigation, the agency found that the Morgan Stanley employee was able to access the client account information in spite of these policies because of improperly configured access controls for a "narrow set of reports." Another factor influencing the agency's decision to close the investigation was the fact that that Morgan Stanley quickly fixed these improper configurations when they were brought to its attention.

As is customary, the FTC's closing letter noted that the decision to close its investigation should not be taken to mean that a violation of Section 5 did not occur, and the FTC reserved the right to take further action against the company.

Implications

The FTC tends to confidentially close privacy and data security investigations, without informing the public as to the existence of the investigation or why it was closed. When the FTC chooses to issue a public closing letter, it often does so to send a specific message or lesson to industry. The Morgan Stanley closing letter offers several takeaways:

- Companies must consider not only external risks to the company but internal risks as well. While much attention is given to the risks of malicious attacks from hackers, 54 percent of breaches last year were caused by human error and system glitches. All three factors were at play in the Morgan Stanley data breach.

- The FTC has long emphasized that companies should identify and address reasonably foreseeable internal risks that could result in a breach, and the closing letter offers insights into what risk mitigation efforts the FTC will consider when weighing whether to close an investigation. First and foremost, companies should implement policies limiting employee access to only the personal information for which they have a business need. If employees don't need information to do their jobs, they shouldn't have access to it. Second, when appropriate in light of a company's size, complexity, and nature of the data handled, a company should establish both administrative policies and technical measures to limit or prevent employees' transferring of personal information, including using tools to monitor the size and frequency of data transfers by employees, prohibiting employee use of USB and similar devices for transferring information, and blocking employee access to certain high-risk websites and applications.

- Companies must promptly address security issues when they come to companies' attention. In closing the investigation, the FTC was influenced by the fact that Morgan Stanley, once aware of how the unauthorized access took place, took quick action to address the weaknesses in its security measures.

The FTC's closing letter and accompanying blog post reiterate that reasonable security is an "ongoing process" and changes over time based on current risks and technologies.[3] As employees increasingly use personal websites and applications in the workplace, companies should implement appropriate controls to address the risk of broad employee access to information.[4]

---

[2] *See* Justin Baer, "U.S. Shifts Focus of Morgan Stanley Breach Probe," *The Wall Street Journal*, February 18, 2015, http://www.wsj.com/articles/u-s-shifts-focus-of-morgan-stanley-breach-probe-1424305501 (last visited Aug. 24, 2015).

[3] Lesley Fair, "Letter to Morgan Stanley Offers Security Insights About Insiders," FTC Business Blog, August 10, 2015, https://www.ftc.gov/news-events/blogs/business-blog/2015/08/letter-morgan-stanley-offers-security-insights-about.

[4] *Id.*

HHS Updates Guide to Protecting Electronic Health Information

Wendy Devine
Associate, San Diego
wdevine@wsgr.com

Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

The Department of Health and Human Services (HHS) Office of the National Coordinator for Health Information Technology (ONC) recently released a practical guide designed to help healthcare providers and their service providers better understand and implement privacy and security protections for electronic health information.[1] Organizations that handle personal health-related information, even when they are subject to HIPAA regulation, may find the HHS guide to be a source of information on emerging and better practices. This is updated guidance following HHS's substantial changes to HIPAA regulations through the omnibus rule in early 2013.

The new guide counsels that the benefits from digital health records rely heavily on cultivating patients' trust that information will be maintained accurately, that patients will have the ability to request access to such data, and that providers and others will carefully handle the information. The guide makes clear that providers are responsible for protecting the confidentiality, integrity, and availability of health information; and that such responsibility is not outsourced to third-party vendors who manage and maintain health information.

HIPAA Compliance

The HHS guide reminds organizations regulated by HIPAA (i.e., covered entities and business associates) that they must comply with the Privacy, Security, and Breach Notification Rules. Generally, business associates are organizations that have access to protected health information (PHI) to perform certain functions or activities on behalf of covered entities, such as healthcare providers, insurance companies, or other business associates. The guide also provides an overview of the HIPAA Privacy, Security, and Breach Notification Rules.

Meaningful Use Programs

The guide describes the Stage One and Stage Two core objectives that address privacy and security with respect to the Medicare and Medicaid Electronic Health Record Incentive Programs ("Meaningful Use" programs). The Meaningful Use requirements align with many HIPAA privacy and security requirements for electronic PHI.

Seven Steps for Security Management

To help organizations meet some of their HIPAA and Meaningful Use program obligations, the guide describes a sample seven-step approach to beginning implementation of a security management process. The steps include:

1. Lead Your Culture, Select Your Team, and Learn
2. Document Your Process, Findings, and Actions
3. Review Existing Security of electronic PHI (Perform Security Risk Analysis)
4. Develop an Action Plan
5. Manage and Mitigate Risks
6. Attest for Meaningful Use Security-Related Objective
7. Monitor, Audit, and Update Security on an Ongoing Basis

Step One: Lead Your Culture, Select Your Team, and Learn

The guide lists several actions that organizations may perform to emphasize protecting patient information as part of their culture. For example, an organization can designate a security officer, use third parties to help perform security risk assessments, and update and republish internal HIPAA training and policies and procedures.

Step Two: Document Processes, Findings, and Actions

Documentation of HIPAA-related policies and procedures is required under HIPAA. The guide states that written documentation also can aid in increasing the efficiency of security procedures, make policies and procedures more accurate and easier to follow, and provide explanation of how security decisions are made and thereby support future decision-making when changes to systems or the risk environment occur.

Step Three: Review Existing Security of Electronic PHI

Organizations regulated by HIPAA that maintain PHI are expected to assess potential threats and vulnerabilities to the confidentiality, integrity, and availability of the information. According to the HHS guide, comprehensive risk assessments should:

- identify where PHI exists and how it is created, received, maintained, and transmitted;
- identify potential threats and vulnerabilities to PHI; and
- identify risks and their associated threat levels based on the likelihood the threat will exploit a vulnerability and the potential resulting impact of such exploitation.

Step Four: Develop an Action Plan

Following a risk analysis, the guide suggests that organizations discuss and develop an action plan to mitigate the identified risks. ONC recommends that organizations begin by identifying the easy actions that can reduce the greatest risks. The HIPAA Security Rule provides flexibility by permitting

[1] Department of Health and Humans Services, Office of the National Coordinator for Health Information Technology, "Guide to Privacy and Security of Electronic Health Information," April 2015, http://healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

Continued on page 13...

HHS Updates Guide . . . *(continued from page 12)*

compliance efforts that take into account the characteristics of the organization and its environment. The guide states that an action plan should have five components:

- Administrative safeguards
- Physical safeguards
- Technical safeguards
- Organizational standards
- Policies and procedures

Step Five: Manage and Mitigate Risks

The guide suggests building an organizational culture that values patients' health information and actively protects it. To help create this culture, the guide recommends implementing the action plan developed in Step Four, training the organization's workforce, implementing and monitoring compliance with policies and procedures, sending regular reminders to the workforce about data privacy and protection, communicating with consumers/patients about the precautions the organization takes with respect to PHI, responding quickly and accurately to patient data requests, and updating contracts with service providers.

Step Six: Attest to Meaningful Use Security-Related Objective

Organizations participating in Meaningful Use programs may consider attesting that they have met the Meaningful Use requirements for a certain reporting period.

Step Seven: Monitor, Audit, and Update Security on Ongoing Basis

The guide recommends that organizations routinely monitor the adequacy and effectiveness of their security infrastructure and make any necessary improvements. The auditing can be done internally and/or with third-party consultants. The guide also suggests that organizations examine historical activity through retrospective documentation (e.g., logging). This type of monitoring can help an organization measure the effectiveness of security controls, such as data tampering resistance, user access and authorizations, automatic log-offs, and emergency access.

For organizations required to comply with HIPAA and those that have made attestations of compliance with Meaningful Use programs, non-compliance can lead to substantial penalties. The guide provides a helpful overview of regulatory requirements and some practical compliance advice that are useful in implementing good faith efforts at compliance. Indeed, compliance with, at a minimum, the recommendations found in the guide may serve as evidence of such good faith efforts of taking steps to comply with the HIPAA Privacy, Security, and Breach Notification Rules. Moreover, given the continued growth of health-tech and headline grabbing breaches involving health-related information, organizations handling such information may find the guide to be a useful resource in evaluating and critically analyzing their security practices. Similarly, any organization considering implementing a security management program or updating an existing program may find the guide to be helpful as a starting point.

Personal Data, Anonymization, and Pseudonymization in the EU

Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com

Sára Hoffman
Associate, Brussels
shoffman@wsgr.com

De-identification techniques are often at the forefront of companies' concerns when it comes to the processing of big data. In addition, anonymization and pseudonymization techniques have been a heavily debated topic in the ongoing reform of EU data protection law. This makes last year's Article 29 Working Party (WP29) Opinion on Anonymization Techniques[1] even more important, as it examines the effectiveness and limits of anonymization techniques and places them in the context of data protection law. This article details the WP29 Opinion on Anonymization Techniques and considers the opinion in relation to the upcoming EU General Data Protection Regulation.

Personal Data, Anonymous Data, and Pseudonymous Data

Under EU data protection law, there are three broad categories of data:

- *Personal data.* The concept of personal data is extremely wide. Personal data is defined as any information relating to an identified or identifiable natural person. 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.[2]
- *Anonymous data.* Anonymous data is any information from which the person to whom the data relates cannot be identified, whether by the company processing the data or by any other

[1] Article 29 Working Party, Opinion No. 05/2014 on Anonymization Techniques, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

[2] Certain personal data receives a higher level of protection under EU data protection because of its sensitivity. As of today, sensitive data includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Continued on page 14...

Personal Data, Anonymization, and Pseudonymization . . . *(continued from page 13)*

person. The threshold for anonymization under EU data protection law is very high. Data can only be considered anonymous if re-identification is impossible, meaning that re-identifying an individual must be impossible by any party and by all means likely reasonably to be used for this attempt. It is an absolute threshold, and the company's intent is not relevant. Anonymized data is no longer considered personal data and is thus outside the scope of EU data protection law.[3]

- *Pseudonymous data.* This concept is not formally defined in the current EU data protection legal framework.[4] Pseudonymization is a form of de-identification, in which information remains personal data. The legal distinction between anonymized and pseudonymized data is its categorization as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data cannot be re-identified.

Anonymization and Pseudonymization Techniques

The processing step of anonymizing personal data is the last legal second that this data falls under the scope of EU data protection laws as personal data. The WP29 opinion considers several anonymization techniques:

- *Noise addition.* This means that an imprecision is added to the original data. For example, a doctor may measure your weight correctly, but after noise addition it shows a weight bandwidth of +/- 10lb.

- *Substitution.* Information values of the original data are replaced with other parameters. For example, instead of indicating a patient's height with 5'7", this value is substituted by the word "blue." If a patient's height is 5'8", it is registered as "yellow." Substitution is often combined with noise addition.

- *Aggregation.* In order not to be singled out, an individual is grouped with several other individuals that share some or all personal data, i.e. their place of residence and age. For example, a data set does not capture the inhabitants of San Francisco with certain characteristics, but the inhabitants of Northern California. *K-anonymity* is a form of aggregation. The process impedes re-identification by removing some information but letting the data be intact for future use. If the scrubbed data set is released and the information for each person contained in the release cannot be distinguished from at least k-1 individuals, it is considered k-anonymous. One method of k-anonymity is data suppression. You can suppress data by replacing a value with a place holder. For example, instead of "age 29," the value is "X." Another method is by generalizing the data. Instead of "age 29," the input is "between 25 and 35." *L-diversity* is an extension of k-anonymity. K-anonymity can be lifted with an interference attack, which allows the attacker to reverse the visible value to the real value. L-diversity protects anonymity by giving every attribute at least *l* different values.

- *Differential privacy.* This comes into play when a company gives a third party access to an anonymized data set. A copy of the original data remains with the company, and the third-party recipient only receives an anonymous data set. Additional techniques such as noise addition are applied prior to the data set transfer. Differential privacy is applied when an authorized third party is requesting data.

Pseudonymization techniques are different from anonymization techniques. With anonymization, the data is scrubbed for any information that may serve as an identifier of a data subject. Pseudonymization does not remove all identifying information from the data but merely reduces the linkability of a dataset with the original identity of an individual (e.g., via an encryption scheme). The WP29 opinion provides the following selected examples of pseudonymization techniques:

- *Hash functions.* Hashes are a popular tool because they can be computed quickly. They are used to map data of any size to codes of a fixed size. For example, the names Cédric Burton, Sára Gabriella Hoffman, and John M. Smith can be hashed to "01," "02," and "03." However long the name, the hash value will always be two digits.

- *Tokenization.* Tokenization is a process by which certain data components are substituted with a non-sensitive equivalent. That equivalent is called the token. The token has no exploitable value, but it serves as an identifier. It is a reference that traces back to the original data.

The WP29 opinion examines the above techniques and categorizes them as follows:[5]

	Is Singling out still a risk?	Is Linkability still a risk?	Is Inference still a risk?
Noise Addition	Yes	May not	May not
Substitution	Yes	Yes	May not
Aggregation	No	Yes	Yes
L-diversity	No	Yes	May not
Differential privacy	May not	May not	May not
Hashing/Tokenization	Yes	Yes	May not

[3] Recital 26 of the EU Data Protection Directive excludes anonymized data from EU data protection law. It reads: "Whereas the principles of protection must apply to any information concerning an identified or identifiable person; (...); whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable (...)".

[4] With the exception of a few national data protection laws, such as German law.

[5] Article 29 Working Party, Opinion No. 05/2014 on Anonymization Techniques, Table 6. Strengths and Weaknesses of the Techniques considered.

Continued on page 15...

Personal Data, Anonymization, and Pseudonymization . . . *(continued from page 14)*

On average, differential privacy scores the highest as an anonymization technique under EU data protection law. However, depending on the concrete risk to be mitigated, one technique may prevail over the other.

Ongoing Discussions and Likely Trends

In the context of the ongoing reform of EU data protection law, the concepts of personal data, anonymous data, and pseudonymized data have been strongly debated. While a formal agreement still needs to be reached, the following trends have emerged:

- *The definitions of personal data and anonymous data will remain substantially similar.* EU data protection principles will continue to apply to any information concerning an identified or identifiable person. As is the case today, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the company processing the data or by any other person to identify the individual. EU data protection law will not continue to apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

- *The concept of personal data will be more specific and broadened.* For example, it seems likely that the legislator will create a presumption of qualification of personal data for unique identifiers and explicitly specify in the EU General Data Protection Regulation that online identifiers, location data, and IP addresses are personal data unless companies can demonstrate that the data does not allow identifying individuals (which in practice may be difficult to prove).[6]

- *The concept of pseudonymized data or of pseudonymization will be formally introduced.* Companies de-identifying personal data and using pseudonymized data or pseudonymization techniques will likely benefit from some level of flexibility under EU data protection law, even though the data will still be considered to be personal data and fall under the scope of application of EU data protection law. There are currently some divergences between the various EU institutions involved in the legislative process as to whether the new framework will simply obligate companies to pseudonymize data without clear business incentives, or whether the new framework will include substantial flexibility for companies using pseudonymization techniques. Hopefully, the latter approach will be followed, but this is uncertain.

Conclusions and Next Steps

The WP29 Opinion on Anonymization Techniques is a bridge that helps interpret a legal criterion with applicable technical solutions. It is a valuable piece of legal interpretation that is of practical relevance as this topic remains at the forefront of companies' concern. With technological development and the state of the art methods in steady flux, the opinion also leaves room for interpretation.

The ongoing EU data protection reform will most likely be based on the same core principles and key concepts, including the definition of personal data and anonymous data. The new framework should also formally define pseudonymized data or pseudonymization, and hopefully will provide for strong incentives for companies to de-identify personal data. To anticipate the upcoming change of law, companies should consider identifying the various types of information that they process, and in particular consider reviewing whether their existing de-identification techniques can be considered to be anonymization or pseudonymization techniques and whether new processes to pseudonymize or anonymize the data can be implemented to benefit for more flexibility in the future. Ongoing monitoring of the legal as well as the privacy-engineering environment is necessary to stay within the boundaries of current and upcoming EU data protection law.

---

[6] EU General Data Protection Regulation will also likely broaden the concept of sensitive data and create new categories of data such as biometric or genetic data.

Technical Standards Open New Avenue to EU Data Protection Compliance

Sára Hoffman
Associate, Brussels
shoffman@wsgr.com

Historically, businesses have called for greater connection between the legal requirements of European data protection law and the requirements of information technology standards. The new International Organization for Standardization (ISO) standard for securely processing personal information in cloud computing environments, ISO 27018, could be a significant and major first step toward creating technical standards that take privacy legal requirements into account.[1] While its effects on compliance under the forthcoming EU General Data Protection Regulation (GDPR) remain to be seen, ISO 27018 offers a promising look at what a more harmonized data protection regime might look like.

ISO 27018 is revolutionary because it was designed for user privacy protection. The certification combines legal requirements for data processing with technical criteria for information security systems. The goal of ISO 27018 is to provide a set of uniform security controls to public cloud computing service providers who act as personal data processors. Data processors can certify to their implementation, upkeep, and management of security controls. For globally operating cloud service providers, this certification is an easy and widely accepted signal of compliance. The first service to certify was Microsoft Azure in February 2015.[2] Other Microsoft products to certify include Office 365, CRM Online, and Intune. Dropbox for Business also certified three months later.[3] ISO 27018 is particularly attractive for U.S.-based cloud service providers with a strong EU presence, as ISO 27018 certification provides a good baseline for establishing much needed trust in cloud services in the EU. ISO certification always has been a strong sign of accountability and trustworthiness.

ISO Background

ISO is an independent non-governmental organization that develops international standards, and is the largest standards issuer of its kind. Its members are from 164 standards organizations around the world. Its goal is to provide businesses with common and internationally accepted standards. Businesses can certify to certain ISO standards,[4] which can be helpful for all entities and consumers along the value chain. While ISO standards are not mandatory, ISO certification is a very powerful, globally influential signal that has become a *de facto* market standard in numerous industries.

While ISO develops international standards, it does not get involved in the certification process and does not issue certificates. Rather, external, nationally accredited certification bodies issue certificates according to ISO standards.

ISO 27018 Within the ISO Certification System

All certifications that belong to the ISO 27000-series are also called ISO27k or the Information Security Management System (ISMS) family. The ISMS family covers data privacy and confidentiality, as well as technical security of IT infrastructure. A cornerstone of the ISMS family is ISO 27002, which gives a code of practice for information security management.[5] ISO 27018 is based on ISO 27002, but makes adjustments for the specific risk environment inherent in processing personal data on a public cloud. ISO 27018 has an implementation guide for ISO 27002 controls. Also, ISO 27018 Annex A lists additional controls and guidance for public cloud service providers processing personal data.

ISO 27018 has four main certification objectives:[6]

- *Easing compliance*. It becomes easier for public cloud service providers to comply with data protection laws when they act as personal data processors
- *Transparency*. Transparency amongst cloud service providers is increased. Customers can vote with their feet and select a well-governed and securely run cloud for their services.
- *Lower transaction costs*. Concluding a contract between a cloud-based data processor and a cloud service customer will become easier if the baseline is set by an ISO standard.
- *Customer audit and compliance rights*. Cloud service customers have a way to enforce the upkeep of security standards of the cloud infrastructure. This includes increased physical and logical network security controls on data centers.[7]

---

[1] In August 2014, the ISO adopted ISO 27018, titled "*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*"
[2] See Microsoft Azure announcement dated February 16, 2015: https://azure.microsoft.com/blog/2015/02/16/azure-first-cloud-computing-platform-to-conform-to-isoiec-27018-only-international-set-of-privacy-controls-in-the-cloud/, last accessed August 12, 2015.
[3] See Dropbox' Blog announcement dated May 18, 2015: https://blogs.dropbox.com/business/2015/05/dropbox-for-business-iso-27018/, last accessed August 12, 2015.
[4] ISO certifications are performed by nationally accredited third party certification bodies that can issue certificates according to ISO standards.
[5] ISO 27002 covers topics such as information security policies and their organization, HR security, asset management, access controls, cryptography, securing the physical environment, operational security such as protection from malware and technical vulnerability controls, incident management, and compliance.
[6] ISO 27018, p. vi.
[7] Cloud computing received its name because of the symbol representing a server. When computer scientists visualize a server, it is represented by a circle. Draw many circles next to each other and in overlap to have the representation of a data center, it looks like a cloud.

Continued on page 17...

Technical Standards Open New Avenue . . . *(continued from page 16)*

Personal Data Protection Requirements in ISO 27018

The core objective of the ISO 27018 standard is to protect personal data from a data breach.[8] ISO 27018 includes the following requirements:

- Process as little data as possible. The privacy principle of data minimization or scarcity is mirrored by the consent structure that ISO 27018 requires. Also, cloud service providers must not use personal data for marketing or advertising unless the data subject has explicitly agreed to it. (ISO 27018, Annex A.4.1 and A.5.1)
- Implement technical and organizational security measures, such as prohibiting portable hard drives containing personal data from leaving the processor's facilities. (ISO 27018, No. 6, 9, 11, 12 and Annex A.10)
- Implement encryption techniques to secure personal data transmission channels. (ISO 27018, No. 10)
- Require sub-contractors of the data processor to abide by the same standards as the contracted processor and inform customers about where their data physically resides. Also, allow customers to ask the processor to disclose all subcontractors. (ISO 27018, Annex A.10.12 and A. 11)
- If a data breach occurs, the cloud service provider has notification obligations to communicate the incident clearly and promptly. (ISO 27018, No. 16)
- The cloud service provider must undergo regular third-party audits to keep the certification valid.[9]

Data Protection Laws Overlapping with ISO 27018

Trust in public cloud services has been a constant stumbling stone for cloud service providers in the EU. New laws are forthcoming that set the data protection and privacy standards higher, and ISO 27018 catches this wave and helps with the compliance process. Numerous ISO 27018 certification components such as its consent requirement and breach notification obligations will also become part of the new GDPR. This is a positive development for two reasons. First, the GDPR will directly apply as an EU-wide regulation that does not need national implementation. For internationally operating cloud service providers, this eases legal compliance across EU countries substantially. Second, the certification standard conveniently overlaps with the GDPR. Companies can now use ISO 27018 to signal legal compliance in those overlapping areas.

Nevertheless, this does not mean that ISO 27018 is congruent with the GDPR. ISO 27018 covers the largest scope of privacy and data protection law requirements to date in a certification, but it is limited to data processors. It also leaves crucial data protection law compliance elements out of scope. Outsourcing (e.g., sub-processor agreements) and data transfers outside of the EU (e.g., subscribing to Safe Harbor) remain complex legal issues that must be addressed separately, as ISO 27018 certification does not cover these points.

Conclusion and Outlook

While the U.S. and the EU take very different approaches to regulating data privacy and security, strong signals of reliability, accountability, and compliance have high value in both markets. Aside from being legal requirements, they are also trust-building tools. In today's environment of increasingly large, costly, and frequent data breaches, companies in both jurisdictions are looking for ways to ensure that their data will be held and processed securely and in compliance with relevant laws, rules, and contractual requirements.

The ISO 27018 standard and corresponding certification is an important step toward a more harmonized international data privacy regime. It is a practical and uniformly accepted standard with strong brand recognition and signaling effect. The certification is a commitment that regulators, other businesses, and customers will recognize and reward with greater trust in a cloud provider's service.

---

[8] ISO 27018 defines a data breach as a "compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to protected data transmitted, stored or otherwise processed." ISO 27018, Sec. 3.1, p. 2.

[9] An example is Dropbox's certificate, https://www.dropbox.com/static/business/resources/dropbox-certificate-iso-27018.pdf.

EU Data Protection Regulators Issue Guidance on Drones

Laura De Boel
Associate, Brussels
ldeboel@wsgr.com

On June 16, 2015, the body of European data protection regulators known as the Article 29 Working Party (WP29) issued an opinion[1] which clarifies EU data protection rules in the context of civil drones. The opinion explains how the principles of EU data protection law apply to drones, and provides a list of recommendations for drone manufacturers and operators, regulators and policymakers, and other stakeholders. This article highlights the key takeaways of the WP29 opinion.

Background

The main piece of data protection legislation in the European Union is EU Data Protection Directive 95/46/EC. The directive includes specific rules on how companies can process personal data, extends specific rights to individuals (e.g., the right to be informed of the data processing), provides for data security measures, and sets significant restrictions for the transfer of personal data.

In the context of drones, the WP29 opinion clarifies that images, sound, geolocation data, or other data collected by drones that relates to an identified or identifiable natural person should be considered personal data, and will be protected by Directive 95/46/EC. However, compliance with the directive may be particularly challenging in the context of drones. For instance, WP29 sees a specific risk of a lack of transparency, since it is difficult for individuals to know how their personal data is being processed via a drone, for what purposes, and by whom. WP29 also warns against the excessive collection of personal data via drones, and multipurpose uses of the bulk data collected.

Recommendations

The WP29 opinion provides a list of recommendations for drone operators, and for drone manufacturers to help the operators comply with EU data protection law. It also provides recommendations to policymakers and stakeholders to take measures to make the drone market compliant with EU data protection law. The key takeaways from the opinion are:

- *Security Measures*

  Under Directive 95/4C/EC, personal data must be protected from data breaches by appropriate security measures. WP29 encourages drone manufacturers to work with security experts to address any security vulnerabilities of their drones. WP29 sees a particular vulnerability in the transmission phase, when personal data is transferred from the drone to the base station. Drone manufacturers should also design drones in such a way that operators can delete or anonymize unnecessary personal data as soon as possible after the data has been collected, and set a storage period after which the collected data is automatically deleted.

- *Information to Drone Operators in Packaging*

  WP29 advises drone manufacturers to provide information within the packaging of the drone (e.g., within the operating instructions) relating to the potential intrusiveness of the drone and recalling the need to respect privacy and data protection laws when using the drone. Where local laws prohibit the use of drones in certain areas, manufacturers could provide a link to official maps that indicate the areas where drones are permitted.

- *Notice to Individuals*

  Directive 95/46/EC requires that individuals receive notice that their personal data will be processed. WP29 considers that, for the processing of personal data via drones, notice should be provided via a combination of channels (e.g., signposts, symbols, website). Drones should also be made visible and identifiable from as far as possible (e.g., using flashing lights, bright colors). When in line of sight, the drone operator should be clearly visible and identifiable with signage, so that it is obvious who is responsible for the drone. Drone manufacturers are advised to take these notice requirements into account in the design of their drones.

WP29 advises drone manufacturers to provide information within the packaging recalling the need to respect privacy and data protection laws

- *Privacy by Design and Privacy by Default, Data Protection Impact Assessments*

  EU regulators require companies to build their products and services in a way that allows compliance with EU data protection law (known as the principles of "Privacy by Design" and "Privacy by Default"). For drone manufacturers

[1] See the WP29 Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilization of Drones (WP231), June 16, 2015, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp231_en.pdf.

Continued on page 19...

EU Data Protection Regulators . . . *(continued from page 18)*

this means, for instance, that the drone should be built in such a way that the collection and/or further processing of unnecessary personal data can be avoided (e.g., by automatically blurring faces when images of identifiable persons are not necessary). WP29 also suggests conducting data protection impact assessments to assess the impact of drones on the right to privacy and data protection.

- *Policymakers and Stakeholders to Develop Framework for Drone Use*

  WP29 calls upon policymakers at the EU and national levels to consult with industry representatives to prepare a framework for drone use which includes data protection requirements. For instance, policymakers and stakeholders should develop criteria for data protection impact assessments to be conducted by drone manufacturers and operators. WP29 also recommends that Civil Aviation Authorities work closely with Data Protection Authorities to include data protection requirements into certifications and licenses for drone operators. WP29 also sees a role for codes of conduct, data protection certifications, and privacy seal schemes to increase industry compliance. Finally, WP29 recommends that the European Commission support research and investment for new technologies intended to increase transparency concerning drones, including smart license plates for drones, for example.

Conclusion

In the EU, drones are perceived as particularly privacy-intrusive devices. Some EU member states have already adopted or prepared drone legislation,[2] and there is EU policy in the making which aims to address privacy and security concerns relating to civil drone use.[3] The WP29 opinion articulates the concerns around drones and cautions drone operators to use drones in a way that takes into account EU privacy concerns. For drone manufacturers this means that they should make privacy- friendly design choices that allow drone operators to comply with EU data protection law.

Some EU member states have already adopted or prepared drone legislation

Although opinions from WP29 are not legally binding, they are taken into consideration by privacy regulators in the EU when applying data protection law. The opinion therefore provides a good indication of how regulators will evaluate compliance of drone manufacturers and operators with data protection and privacy laws in the EU. Moreover, WP29's recommendations (e.g., making privacy-enhancing design choices) are in line with the principles included in the proposed new EU data protection legal framework, i.e., the General Data Protection Regulation.[4]

---

[2] For instance, the Belgian government is preparing drone legislation which recently received the green light from the Belgian Privacy Commission. The Privacy Commission's opinion on this draft legislation is available at http://www.privacycommission.be/sites/privacycommission/files/documents/advies_32_2015.pdf (in Dutch) and http://www.privacycommission.be/sites/privacycommission/files/documents/avis_32_2015.pdf (in French).

[3] The European Aviation Safety Agency is currently seeking input from drone stakeholders to propose a regulatory framework for drone operations. The expiration date for comments is September 25, 2015. More information is available at https://www.easa.europa.eu/newsroom-and-events/news/short-summary-easa%E2%80%99s-proposals-new-rules-drones.

[4] The proposed General Data Protection Regulation is a new piece of EU data protection legislation that is now in the final stages of the EU legislative process. It is expected to be adopted sometime between the end of 2015 through the beginning of 2016. The General Data Protection Regulation would become effective two years after adoption. For an update on the latest developments concerning the regulation, please see the July 2015 issue of the WSGR Data Advisor at: https://www.wsgr.com/publications/PDFSearch/the-data-advisor/Jul2015/index.html#4.

Upcoming WSGR Privacy & Data Protection Events

The Future of Privacy in a Connected World: A Cross-Border Conversation
September 16, 2015, 3:00 p.m. – 6:30 p.m. PDT
Garden Court Hotel, Palo Alto

- WSGR will host a discussion with key policymakers in the United States and the European Union on global privacy and data protection. The panel will be moderated by Lydia Parnes and Christopher Kuner. Panelists include Julie Brill, Commissioner of the U.S. Federal Trade Commission (FTC); Giovanni Buttarelli, European Data Protection Supervisor (EDPS); and R. David Edelman, Special Assistant to the President for Economic and Technology Policy, The White House.

Upcoming Industry Events Featuring WSGR Privacy & Data Protection Professionals

IAPP Privacy Academy and CSA Congress
September 29 - October 1
Las Vegas

- WSGR partner Lydia Parnes will moderate a keynote panel on October 1 featuring Jessica Rich and Travis LeBlanc, the lead enforcers at the FTC and FCC, who will discuss their complementary roles in regulating the rapidly growing and evolving tech industry in the U.S. Also on October 1, WSGR Of Counsel Tracy Shapiro will moderate a panel discussing what companies should to do to ensure that their mobile advertising and data collection efforts comply with DAA guidance.

American Bar Association Forum on the Entertainment and Sports Industries
October 8-10
Washington, D.C.

- WSGR partner Lydia Parnes will moderate a panel discussion on October 8 addressing the "Sony Hack" and other key issues resulting from mass data collection and data breaches of personal information.

- WSGR partner Gary Greenstein will moderate a breakfast roundtable on October 9 examining U.S. Department of Justice consent decree reform.

2015 IAPP Europe Data Protection Congress
December 2-3
Brussels

- WSGR partner Michael Rubin will moderate a panel at the annual conference for international privacy and data protection professionals. More details will be announced soon.

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

650 Page Mill Road, Palo Alto, California 94304-1050 | Phone 650-493-9300 | Fax 650-493-6811 | www.wsgr.com

Austin Beijing Brussels Hong Kong Los Angeles New York Palo Alto San Diego San Francisco Seattle Shanghai Washington, DC Wilmington, DE