

Welcome

With a new year come exciting new developments in the world of privacy and data protection. We are thrilled to announce the launch of the digital version of *The WSGR Data Advisor*. Please visit www.wsgrdataadvisor.com for the latest news and an archive of past articles. Our new site makes it easier to browse and search all of our articles and provides a venue for us to cover emerging developments between issues.

In this issue of *The WSGR Data Advisor*, we examine the political agreement recently reached by the European Parliament and the Council of the European Union on the text of the EU General Data Protection Regulation; we present a comparison and key takeaways from the FCC's Open Internet Order and the EU's Network Neutrality Regulation for players in the telecommunications sector; and we examine the FTC's recent approval of a new facial recognition method to obtain parental consent to collect children's personal information.

In addition, we examine several privacy- and security-related provisions of the FAST Act, which was recently signed into law; we discuss new cybersecurity and incident notification rules in the EU; and we highlight three HIPAA non-compliance settlements announced by the U.S. Department of Health and Human Services in late 2015.

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. And please make sure to visit www.wsgrdataadvisor.com for the latest updates between issues.

Lydia Parnes & Michael Rubin
Wilson Sonsini Goodrich & Rosati



Lydia Parnes

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



Michael Rubin

Michael Rubin
Partner, San Francisco
mrubin@wsgr.com

EU Reaches Political Agreement on New Data Protection Regulation



Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com



Laura De Boel
Associate, Brussels
ldboel@wsgr.com

On December 15, 2015, the European Parliament and the Council of the European Union reached a political agreement on the text of the EU General Data Protection Regulation (GDPR).¹ This is a major step toward the official adoption of the GDPR, which is now expected in Spring 2016. The GDPR will have a significant impact on how EU and non-EU businesses can collect and process the personal data of EU individuals.

This article discusses the key elements of the GDPR.

Background

The review process started four years ago, in January 2012,² when the European Commission introduced its proposal for the GDPR. Both the European Parliament and the Council proposed their own version of the GDPR (in March 2014³ and June 2015,⁴ respectively) and, on that basis, negotiated a compromise text. This compromise text is now being finalized by the EU's legal services, meaning that it may still undergo some final changes. However, the version of the GDPR agreed to on December 15, 2015, can be regarded as very close to the final text. We refer to that version in this update.

In This Issue

EU Reaches Political Agreement on New Data Protection Regulation Pages 1-3

The FCC's Open Internet Order and the EU's Network Neutrality Regulation: A Comparison and Key Takeaways for Players in the Telecommunications Sector..... Pages 4-7

FTC Approves Facial Recognition as Method of Obtaining Parental Consent to Collect Children's Information . Pages 8-10

FAST Act Eases GLBA Compliance Burdens for Many Companies, Addresses Transportation and Infrastructure Privacy and Cybersecurity Issues..... Pages 10-11

EU Agrees to New Cybersecurity and Incident Notification Rules..... Pages 12-13

HHS Ends 2015 with Three HIPAA Enforcement Settlements..... Pages 14-15

¹The compromise consolidated text of the GDPR (outcome of the Trilogue on December 15, 2015) is available at: [http://www.emeeting.europa.eu/committees/agenda/201512/LIBE/LIBE\(2015\)1217_1/sitt-1739884](http://www.emeeting.europa.eu/committees/agenda/201512/LIBE/LIBE(2015)1217_1/sitt-1739884).

²See the Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), COM (2012) 11 final (January 25, 2012), http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

³See the European Parliament legislative resolution of March 12, 2014, on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+X-ML+VO//EN>.

⁴See Council document no. 9565/15, adopted as its "General Approach" at: <http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf>.

EU Reaches Political Agreement on New Data . . . *(continued from page 1)*

Key Elements of the GDPR

The GDPR will replace EU Data Protection Directive 95/46/EC, which is currently the main legal framework for data protection in the EU. The GDPR's provisions are far-reaching and have sparked intense debate and lobbying throughout the legislative process. Below are some of the most important elements of the GDPR.

- *Extraterritorial Effect.* The GDPR will apply to organizations established in the EU, but also to non-EU organizations collecting and processing the personal data of EU individuals to offer them goods and services (e.g., via a website), freely or against payment, or to monitor their behavior (e.g., by tracking individuals online to build profiles). Thus, nearly all non-EU businesses that are active in the EU will be subject to the strict requirements of the GDPR.
- *Concept of Personal Data and Sensitive Data.* The GDPR maintains the current definition of personal data (i.e., data relating to an identified or identifiable natural person), but provides more examples of data that can qualify as personal data, such as location data and online identifiers (e.g., IP addresses, cookies). Under the GDPR, as under the current Data Protection Directive, sensitive types of personal data will receive specific protection. The GDPR adds genetic data and biometric data to the group of sensitive data.
- *Consent and Other Legal Grounds for Processing.* The GDPR will add more restrictions to the legal grounds for processing personal data. In particular, the GDPR adds conditions for consent to be a valid ground for data processing. For instance, consent must be obtained via a specific (i.e., separate from general

terms) and clear consent statement. The GDPR also introduces rules for parental consent for the processing of children's personal data in the context of information society services offered directly to children. Parental consent will be required if the child is under 16, unless national law in the relevant EU country sets a lower age limit (provided the limit is not below the age of 13). Companies will be expected to take reasonable efforts and to use available technology to verify that parental consent has been duly obtained.

- *New Accountability Requirements.* The GDPR will replace the current requirement to submit filings with Data Protection Authorities (DPAs) by a new requirement to maintain internal documentation on the company's data processing activities. In addition, companies will need to conduct privacy impact assessments if they conduct high-risk data processing activities, and in particular if they: (i) profile individuals; (ii) process sensitive data on a large scale; or (iii) systematically monitor a publicly accessible area on a large scale. Companies will also be required to implement privacy-enhancing measures when they design their products and services (privacy by design) and to, by default, select the techniques that are the most protective of individuals' privacy and data protection (privacy by default). If a company's core data processing activities involve the monitoring of individuals on a large scale or encompass sensitive data, the company will also be required to appoint a data protection officer.
- *New Obligations for Service Providers Acting as Data Processors.* The GDPR will impose many more restrictions on the outsourcing of data processing

activities to data processors. The current requirement for data processors to protect personal data with appropriate security measures will be complemented by specific obligations that must be included in data processing agreements, such as requirements to obtain the data controller's prior written approval for subprocessors; to contractually impose the same obligations on subprocessors as are imposed on the data processor; and to assist the data controller in ensuring data protection compliance.

- *New Data Breach Notification Requirement.* The GDPR introduces a personal data breach notification requirement. Under the GDPR, a data breach will have to be reported to the national DPA if it is likely to result in a risk for the rights and freedoms of individuals. The data breach will have to be reported to the DPA without undue delay, and when feasible, within 72 hours after a company becomes aware of the breach. The data breach will also need to be reported to the individuals concerned, without undue delay, if it is likely to result in high risks, unless certain exceptions apply (e.g., the data is encrypted, the company has taken measures to reduce the risks). The introduction of a pan-EU general data breach notification requirement is an important novelty under EU data protection law. Guidance regarding the circumstances in which companies are required to notify data breaches will be issued by the European Data Protection Board (EDPB), which is a new EU body that will gather all national DPAs and replace the existing Article 29 Working Party.
- *New Rights for Individuals.* The GDPR strengthens the current rights of individuals under the Data Protection Directive, and also includes a few

Continued on page 3...

EU Reaches Political Agreement on New Data . . . *(continued from page 2)*

new rights. The GDPR codifies the “right to be forgotten,” which was affirmed by the Court of Justice of the EU in its *Costeja* decision in 2014.⁵ The new “right to data portability” further strengthens individuals’ control over their personal data by allowing them to export personal data from one controller to another, without hindrance. Controllers will thus need to use interoperable formats when handling personal data.

- *International Data Transfers.* The GDPR will broadly maintain the current rules on international data transfers: personal data may only be transferred to a country that has been considered to provide an “adequate level of data protection,” unless the company has implemented a data transfer mechanism or can rely on a statutory derogation. The GDPR provides new criteria for a country to be considered “adequate”; some of which are clearly imported from the judgment of the EU Court of Justice in *Schrems*⁶ that invalidated the “adequacy” decision for the U.S.-EU Safe Harbor program for data transfers. Any new agreement between the U.S. and the E.U., such as a Safe Harbor 2.0, would have to meet these requirements. Importantly, current EU model contracts and DPA authorizations for Binding Corporate Rules and ad-hoc contracts will remain valid, until amended, replaced, or repealed by the EU Commission or DPAs.

In addition, the GDPR introduces new data transfer mechanisms, such as adherence to approved codes of conduct or approved certification mechanisms. These mechanisms still need to be developed, and it remains to be seen whether they will prove

to be useful in practice, but these are interesting additions to the tools available for data transfers.

The GDPR keeps the statutory derogations for international data transfers that are included in the Data Protection Directive (e.g., individual’s consent, execution of a contract), but adds a new derogation for data transfers: the controller’s compelling legitimate interests (provided that they are not overridden by the interests or rights and freedoms of the individual). However, this new derogation is subject to strict conditions: the transfer must not be repetitive, concerns only a limited number of individuals, and the controller must adduce suitable safeguards to protect the data and inform the individuals concerned.

- *One-Stop Shop, Cooperation Procedure, and Consistency Mechanism.* For companies that are active in multiple EU countries, the GDPR will to a certain extent centralize data protection enforcement. The GDPR introduces a “one-stop shop” mechanism through which the DPA of a company’s main establishment in the EU will take the lead in supervising a company’s compliance across the EU. Other DPAs involved will need to cooperate with the lead DPA through a newly created cooperation procedure. To further ensure consistent application of the GDPR in the EU and to solve disagreements between the lead DPA and other DPAs, the GDPR also creates a consistency mechanism under the authority of the EDPB.
- *Higher Fines and Harmonization of DPA Enforcement Powers.* The GDPR is designed to step up data protection enforcement in the EU.

The GDPR introduces high fines for non-compliance with the new rules. There will be a two-tiered system of fines. The first level, for less severe violations, is set at maximum €10 million or 2 percent of the undertaking’s global annual turnover, whichever is higher. The second level, for more severe violations, is set at maximum €20 million or 4 percent of the undertaking’s global annual turnover, whichever is higher. Moreover, the enforcement powers of DPAs, such as the power to conduct investigations and audits, will be harmonized. The cooperation of DPAs will also be strengthened to ensure the consistent application and enforcement of the GDPR throughout the EU.

Next Steps

It is now almost certain that the GDPR will be adopted by Spring 2016. It will enter into force two years after its adoption—i.e., by Spring 2018. Companies should begin to assess how their business activities will be impacted by the forthcoming GDPR. This means taking stock of the company’s data protection practices, policies, procedures, and contracts to analyze compliance gaps under the GDPR. The two-year transition period might seem long, but for many companies it will be a time-consuming effort to adapt business practices to the requirements of the GDPR.

For a more detailed analysis, please see our recent article in Bloomberg BNA, and to keep up to date with the legislative developments concerning the GDPR, see Wilson Sonsini Goodrich & Rosati’s EU Data Protection Regulation Observatory at <https://www.wsgr.com/eudataregulation/>.

⁵See the CJEU Judgment, delivered on May 13, 2014, in Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=152065&occ=first&dir=&cid=276746.

⁶See the CJEU Judgment, delivered on October 6, 2015, in Case C-362/14 Maximilian Schrems v. Data Protection Commissioner (request for a preliminary ruling from the High Court (Ireland)), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=1&part=1&mode=req&docid=169195&occ=first&dir=&cid=111628.

The FCC's Open Internet Order and the EU's Network Neutrality Regulation: A Comparison and Key Takeaways for Players in the Telecommunications Sector



Brian Willen
Partner, New York
bwillen@wsgr.com



Sára G. Hoffman
Associate, Brussels
shoffman@wsgr.com

The Internet has transformed the ways that we access, consume, and use information. For years, debates have raged in both the United States and Europe over so-called “network neutrality”—the extent to which the government should require entities that provide Internet access services to treat the content that they transmit equally. In the past several months, there have been significant events with regard to network neutrality laws in the U.S. and the EU. Regulators in both jurisdictions have promulgated sweeping rules that impose new obligations on companies that operate in the telecommunications sector. This article provides an overview and high-level comparison of the new legal framework in both jurisdictions, and offers some key takeaways for companies affected by network neutrality laws on both sides of the Atlantic.

Regulators in the U.S. and the EU have promulgated sweeping rules that impose new obligations on telecommunications companies

The FCC's Open Internet Order

On February 26, 2015, the Federal Communications Commission (FCC) adopted its Open Internet Order, a comprehensive regulation to foster market access to the Internet and to prohibit Internet service providers (ISPs) from favoring certain types of content. In particular, the FCC order prohibits ISPs from: (i) blocking access to legal content, applications, services, or non-harmful devices; (ii) throttling lawful Internet traffic on the basis of content, applications, services, or non-harmful devices; and (iii) receiving payment (or other consideration) for favoring or prioritizing particular content. In addition to these bright-line rules, the FCC also adopted a general “no unreasonable discrimination” standard for ISPs.

At the same time, however, the FCC qualified some of these rules by embracing the concept of “reasonable network management.” Tools and practices falling into this category allow broadband service providers to “optimize overall network performance and maintain a consistent quality experience for consumers while carrying a wide variety of traffic over their network.” The FCC has defined “reasonable network management” as:

“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.”

Reasonable network management is an exception from the bans on blocking and throttling (but not paid prioritization). Because the FCC's definition is rather open-ended, its particular application will have to be fleshed out on a case-by-case basis.

But the FCC's regulatory reach went further than these core issues. Two other key changes are new rules governing common carriers and the regulation of mobile broadband services:¹

- *Reclassification of ISPs.* The FCC's Open Internet Order reclassified ISPs from “telecommunication services” to “common carriers.” This gives ISPs the same regulated status as held by providers offering traditional landline telephone services, though the FCC has indicated that it will forebear from enforcing most of the rules that apply to other common carrier, including rate regulation.
- *Regulation of Mobile Broadband.* The new order applies the open Internet rules to mobile as well as fixed broadband providers. Previously, the FCC had excluded mobile services from several network neutrality provision, sheltering a more immature market.

The FCC has argued that these principles will help preserve and protect the “‘virtuous cycle’ in which innovations at the edges of the network enhance consumer demand, leading to expanded investments in broadband infrastructure that, in turn, spark new innovations at the edge.”²

The FCC's order is now under legal challenge with the U.S. Court of Appeals for the District of Columbia. The challengers argue that the

¹For a detailed analysis of the FCC's defense of its Open Internet Order, see WSGR Alert, “Five Things to Know about Net Neutrality,” December 10, 2015, <https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-net-neutrality.htm#2>.

²In the Matter of Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, Docket No. 14-28. The full text is available here: <https://www.fcc.gov/document/fcc-releases-open-internet-order>.

Continued on page 5...

The FCC's Open Internet Order and the EU's Network . . . *(continued from page 4)*

order violates the FCC's statutory authority and the First Amendment, as that it was procedurally improper. Until the court renders its judgment, the FCC's Open Internet Order remains fully in effect.

The EU's New Network Neutrality Regulation

Legislative Process

In comparison to the U.S., this is the first time the EU has adopted an EU internal market-wide rule for network neutrality.³

In the EU, the lawmaking process involves the European Parliament, the European Council, and European Commission. The trilogue negotiations between these EU institutions ended on June 30, 2015. On that day, the European Parliament and the European Council reached an agreement on the compromise text of new rules to end mobile phone roaming fees and to safeguard open Internet access, the latter also known as network neutrality rules.⁴

The new laws, which include provisions on roaming and network neutrality, entered into force three days after its publication in the Official Journal of the European Union, on November 29, 2015.⁵ However, the provisions governing network neutrality have an implementation grace period. Those provisions will enter into effect after April 30, 2016. This gives the private sector a few months to adjust to the new legal framework.

Key Material Provisions

The new provisions establish common rules to safeguard "equal and non-discriminatory treatment of traffic in the provision of Internet access services." When providing Internet access services, providers shall "treat all traffic equally, without discrimination, restriction or interference, independently of its sender or receiver, content, application or service, or terminal equipment."⁶

Traffic prioritization follows a two-step assessment. First, paid and non-paid traffic prioritization is distinguished. Paid traffic prioritization is prohibited *per se*. Second, the rules differentiate between allowed and prohibited types of non-paid traffic prioritization.

Non-paid prioritization is only allowed if (i) the prioritization is independent of the origin and destination of traffic and (ii) one of the following narrow exceptions applies:

- specific content that has been deemed illegal by e.g., a court order or public authorities can be blocked from transmission;
- traffic may be prioritized to preserve the security and integrity of the network because the network is being misused or viruses, malware or denial of service attacks. Measures that fend off these attacks fall under the exception; or

In comparison to the U.S., this is the first time the EU has adopted an internal EU market-wide rule for network neutrality

- the prioritization serves minimizing temporary or exceptional network congestions. This exception cannot be invoked if the network is frequently congested due to underinvestment in the network and constant capacity scarcity.

Traffic management measures are not considered prioritization. They are exempt from the rules governing traffic prioritization if they serve the purpose of grid maintenance, contribute to an efficient use of network resources, or optimize overall transmission quality. The EU Network Neutrality Regulation describes them as follows:

"Reasonable traffic management measures applied by providers of Internet access services should be transparent, non-discriminatory and proportionate, and should not be based on commercial considerations. The requirement for traffic management measures to be non-discriminatory does

³Within the EU, only Slovenia and The Netherlands have national network neutrality laws. Both countries have adopted their legislation in 2012. France and Belgium are currently working on legislative proposals, but do not have a national legal framework in place yet. See the French proposal (in French) here: <https://www.republique-numerique.fr/pages/projet-de-loi-pour-une-republique-numerique> and the Belgian proposal (in Dutch and French) here: <http://www.dekamer.be/FLWB/pdf/53/1467/53K1467001.pdf>

⁴The press release is available here: <http://www.consilium.europa.eu/en/press/press-releases/2015/06/30-roaming-charges/>.

⁵The position of the European Council titled "Position of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No. 531/2012 on roaming on public mobile communications networks within the Union" (EU Network Neutrality Regulation) was adopted in its final version without further amendments. The Council's version is available here: <http://data.consilium.europa.eu/doc/document/ST-10788-2015-INIT/en/pdf>.

⁶Recital No. 8 EU Network Neutrality Regulation.

Continued on page 6...

The FCC's Open Internet Order and the EU's Network . . . *(continued from page 5)*

not preclude providers of Internet access services from implementing, in order to optimize the overall transmission quality, traffic management measures which differentiate between objectively different categories of traffic. Any such differentiation should (...) be permitted on the basis of objectively different technical quality of service requirements (for example, in terms of latency, jitter, packet loss, and bandwidth) of the specific categories of traffic, and not on the basis of commercial considerations.”⁷

The EU rules also harbor a privilege for “specialized services.” Specialized services are services that are different from—and are provided in addition to—the open Internet access services. They have specific quality requirements for specific content, applications, or services. Examples include IPTV, high-definition video conferencing, and healthcare services, including telesurgery. Specialized services have higher technical requirements that “cannot be ensured in the best-effort open Internet.” They may receive (non-paid) prioritized treatment if that is objectively necessary for the service and is narrowly tailored. ISPs in the EU would be required to provide enough capacity so that specialized services can be offered without slowing down general Internet access.

Network Neutrality Laws Compared

While the EU and FCC rules aim to advance similar goals, they do so in different ways. The EU laws focus primarily on Internet traffic management and incorporate detailed rules and examples describing the fairness, non-discrimination and transparency elements. The rules are very concise and only encompass two core sections, i.e., three pages. The narrow focus is illustrated by the fact that the provisions are part

of a legislative package covering mobile telephone roaming charges—relating to mobile telecommunication services traffic management.

In comparison, the FCC rules are much more detailed and laid out in more than 400 pages. The rules address ISPs, Internet traffic exchange, non-broadband Internet access

While the EU and FCC rules aim to advance similar goals, they do so in different ways

services, data services, and reasonable network management rules in a more nuanced fashion.

The key similarities and differences are the following:

- *No Blocking and Throttling.* Under the FCC rules, ISPs are prohibited from blocking lawful content, applications, services, or non-harmful devices, unless they are engaged in reasonable network management. There is a separate (but largely parallel) ban on throttling, which is designed to avoid efforts to evade the no-blocking rule by rendering an application effectively, but not technically, unusable. The FCC’s no-throttling rule specifically prohibits actions that single out content competing with the service provider’s own business.

The EU Network Neutrality Regulation does not provide stand-alone rules

for blocking and throttling. Instead, the EU has adopted a general rule prohibiting “any traffic management practices which go beyond reasonable traffic management measures, by blocking, slowing down, altering, restricting, interfering with, degrading or discriminating between specific content, applications or services, or specific categories of content, applications or services, should be prohibited, unless a justification or exception applies.”

The gist of the US and EU blocking and throttling rules is similar, however. In both jurisdictions, network operators are barred from blocking and/or throttling lawful content, subject to a somewhat open-ended exception reasonable network or traffic management. The EU rule also has a general “justification” exception, which may operate as a safety valve that is missing from the more rigid FCC rule.

- *No Paid Prioritization.* The FCC’s Open internet Order entails a blanket prohibition on accepting payment or any other form of consideration for traffic prioritization. The EU’s approach to network neutrality is very similar: paid traffic prioritization is prohibited *per se*. There is no exception from these rules in either jurisdiction for “reasonable” network or traffic management. Such measures simply cannot take the form of paid priority lanes.
- *No Unreasonable Discrimination.* Both the FCC and the EU have a general prohibition on ISPs unreasonably discriminating between different content or applications on their

⁷Recital No. 9 EU Network Neutrality Regulation.

Continued on page 7...

The FCC's Open Internet Order and the EU's Network . . . *(continued from page 6)*

networks. In the EU, this is simply one aspect of the general rule; in the US, it is a broad (but more ambiguous) catch-all limit on forms of discrimination beyond blocking, throttling, and paid prioritization that ISPs might try to use to favor some content over others. In both jurisdictions, interesting questions arise about what may be covered by this prohibition; in particular, whether certain kinds of "zero-rating" plans and data caps may be under threat.

In the U.S., the legality of such plans will have to be resolved on a case-by-case basis under the general "no unreasonable discrimination" standard. In the EU, the European Commission has suggested that limits on what it calls "sponsored connectivity" ("a commercial practice . . . not to count the data volume of particular applications or services against the user's limited monthly data volume") are implied in the general non-discrimination requirement.⁸

- **No Altering.** The EU rules ban ISPs from "altering" data transmitted on their networks. There is no parallel prohibition in the FCC rules, though certain alterations may fall within the ban on unreasonable discrimination.
- **Regulatory Perspective.** The EU's angle to network neutrality is strongly rooted in the concepts of consumer protection, transparency, and non-discriminatory access to Internet services. The FCC has also considered these aspects, but places

a comparatively stronger emphasis on the forces of innovation and business needs. Also, the FCC has given much consideration to the effects on the First Amendment aspect of the regulation, an impact assessment that is missing from the EU rules.

- **Enforcement.** The FCC may enforce the Open Internet Order through investigations and the processing of formal and informal complaints, which may ultimately lead to the imposition of fines or other remedial measures. The Enforcement Bureau is authorized to request written opinion from outside technical organizations and obtain additional technical advice from industry standard-setting bodies.

Under the EU rules, national regulatory authorities may impose requirements concerning technical characteristics, minimum quality of service requirements and other appropriate and necessary measures on ISPs. With that, the enforcement of network neutrality laws is left to the EU member states. The Body of European Regulators of Electronic Communications (BEREC) shall issue guidelines on the implementation of the EU Network Neutrality Regulation. Those BEREC communications will be particularly important for the private sector and should be monitored closely. Penalties for violating network neutrality laws will also be determined by the EU member states. The penalties provided for must be effective, proportionate, and dissuasive. Member states shall notify the European Commission of

those rules and measures by April 30, 2016, which is the same day that the laws will enter into effect.

Conclusion

The FCC's Open Internet Order and the EU Network Neutrality Regulation have much in common: both flatly prohibit paid prioritization; and both put substantial limits on blocking, throttling, and other forms of discrimination, subject to tailored exceptions focused on reasonable traffic management measures.

Nevertheless, there are important differences in the approaches that the U.S. and EU regulators have taken, particularly when it comes to enforcement. The EU's approach is more general and leaves considerable room for the EU Commission, BEREC, and the EU member state's national regulators to exercise discretionary powers. Enforcement of the U.S. rules is more centralized with the FCC.

In both the U.S. and the EU, the broad principle of network neutrality has been ratified but there are many questions that remain unanswered. From fleshing out the contours of reasonable network management, to deciding what kind of content and applications are unlawful (and thus outside the rules), to determining whether zero-rating plans and data caps are permissible, both U.S. and EU regulators have their work cut out for them in giving shape to the new rules. In the meantime, companies operating in this space should proceed with caution and seek legal guidance to help manage the uncertainty.

⁸Available here: http://europa.eu/rapid/press-release_MEMO-15-5275_en.htm.

FTC Approves Facial Recognition as Method of Obtaining Parental Consent to Collect Children's Information



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



Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

The Federal Trade Commission (FTC) recently approved a new method for website operators and mobile application developers ("operators") to obtain parental consent to collect personal information from children.¹ Under this new method, which is the first to use biometric identifiers to verify that a parent is providing consent for a child, the FTC will permit operators to use facial recognition technology to compare an image of the person providing consent with an image of verified photo identification, such as a drivers' license or passport. If the two images match, the user is verified and can provide consent for the child to use the website or mobile application.

COPPA Requirements to Collect Personal Information from Children Under 13

Generally, under the FTC's COPPA Rule, before a website, app, or online service collects personal information from children under 13, it must:

1. provide proper notice of its practices with regard to the collection, use, or disclosure of personal information from children directly to parents and on its website, and
2. obtain verifiable parental consent to its privacy practices.

Verifiable Parental Consent

COPPA requires an operator to make "reasonable efforts to obtain verifiable parental consent, taking into consideration available technology. Any method to obtain verifiable parental consent must be reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent."² COPPA delineates specific, existing methods of obtaining verifiable parental consent that

COPPA requires an operator to make reasonable efforts to obtain verifiable parental consent, taking into consideration any available technology

satisfy the foregoing standard, including a signed consent form, a monetary transaction, a telephone or video-conference call, or checking a form of government-issued identification against databases of such information.³ COPPA also allows interested parties to file a written request for FTC approval of parental consent methods not specifically laid out in the rule, in order to encourage the development of new consent methods that provide businesses with more flexibility while ensuring that parents are providing consent for their children. The FTC has previously approved additional methods of parental consent such as knowledge-based authentication, which uses "out-of-wallet" challenge-and-response questions to

verify that a parent is providing consent.⁴

Requirements for New Methods of Verifiable Parental Consent

For the FTC to accept a proposed verifiable consent method, it must conclude that: (1) the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent; and (2) if there is any risk to consumers' personal information, the risk is outweighed by the benefit to consumers and businesses of using this method.⁵ When the FTC approves a new method, the applicant or any other party can use the method.

FTC Approval Letter for "Face Match to Verified Photo Identification"

On November 18, 2015, the FTC granted an application submitted by Riyo Verified Ltd. seeking approval of its proposed verifiable parental consent method involving facial recognition technology. The new method, "face match to verified photo identification" (FMVPI), combines photo ID verification with facial recognition technology in a two-step process. For the first step, the parent sends a picture of his or her photo identification (e.g., driver's license or passport) to the service performing the verification. The service then verifies the authenticity and legitimacy of the identification document to ensure that it is an authentic government-issued identification.

The second step of proposed FMVPI method involves facial recognition technology. The verification service prompts the parent to take a photo of his or her own face with a phone camera or webcam. The service detects facial movements to ensure this photo is of a live person, rather than a photo of a photo. The image of the parent's face

¹See Commission Letter Approving Application Filed by Jest8 Limited (Trading As Riyo) For Approval of A Proposed Verifiable Parental Consent Method Under the Children's Online Privacy Protection Rule at https://www.ftc.gov/system/files/documents/public_statements/881633/151119riyocoppaletter.pdf.

²16 C.F.R. § 312.5 (b)(1).

³16 C.F.R. § 312.5 (b)(2).

⁴See WSGR Alert, "Websites and Apps Have More COPPA Options," July 23, 2014, at <https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-coppa-options.htm>.

⁵Children's Online Privacy Protection Rule Proposed Parental Consent Method, 80 Fed. Reg. 47429, 47429 (August 7, 2015).

Continued on page 9...

FTC Approves Facial Recognition . . . *(continued from page 8)*

is then compared to the face displayed on image of the photo identification. Photos that do not meet the required level of quality to perform a comparison are rejected. After passing these checks, both images are then reviewed by live agents who are trained to double-check that the photos match. Once the parent is verified, the consent process is completed, and the identification information submitted by the parent is promptly deleted within five minutes.

The FTC concluded that facial recognition algorithms are sufficiently accurate and reliable at one-to-one verification—comparing one image against a second image—to be used to match a photo of a user against a government-issued ID card.⁶

While acknowledging that facial recognition technology is not perfect, the FTC noted that the technology has rapidly improved performance in recent years and is now being used to verify identity by retailers, financial institutions, and technology companies for safety and security purposes. The FTC also pointed out that a second level of review by trained personnel would help to ensure accurate matches. Finally, the FTC found that the risk to personal information was minimized by using the submitted information only to perform the service and then promptly destroying it, and the FTC's approval was conditioned on adherence to these conditions. The FTC also highlighted in its press release that all of the personal information would be encrypted.⁷

Implications

With the FTC's approval of Riyo Verified Ltd.'s application, website operators and mobile application developers have another option for obtaining verifiable parental consent in order to collect personal information from children. For many website operators and mobile application developers, this high-tech option may be more appealing than some of the other lower-tech methods already accepted by the FTC. Operators that choose to implement the FMVPI method, whether in-house or through a service provider, must comply with the conditions described in the FTC's approval letter to ensure that the method is reliable and adequately protects the parents' privacy.

⁶The FTC cautioned that its approval only speaks to one-to-one-matching and declined to opine on any facial recognition method that involves checking a single photo against a database on many photos.

⁷ <https://www.ftc.gov/news-events/press-releases/2015/11/ftc-grants-approval-new-coppa-verifiable-parental-consent-method>.

FAST Act Eases GLBA Compliance Burdens for Many Companies, Addresses Transportation and Infrastructure Privacy and Cybersecurity Issues



Matt Staples
Associate, Seattle
mstaples@wsgr.com



Jon Adams
Associate, San Francisco
jadams@wsgr.com

President Obama signed the Fixing America's Surface Transportation Act (FAST Act) into law on December 4, 2015. The FAST Act not only provides long-term funding for highway and infrastructure improvements and other transportation projects, but also includes several privacy- and security-related provisions, including an important provision that may reduce consumer confusion and industry compliance costs by eliminating annual privacy notice requirements for financial institutions in certain circumstances.

Changes Affecting GLBA Annual Privacy Notices

Under the Financial Services Modernization Act of 1999, better known as the Gramm-Leach-Bliley Act (GLBA), financial institutions must mail an annual privacy notice to their customers that sets forth how they collect, use, and disclose those customers' nonpublic personal information (NPI) and whether customers may limit such sharing. Section 75001 of the FAST Act eliminates this annual notice requirement for financial institutions that satisfy two criteria:

- the financial institution does not share NPI with nonaffiliated third parties except pursuant to certain GLBA exceptions permitting such disclosures (i.e., where sharing occurs in a manner that does not require the financial institution to provide an opt-out right to consumers under the GLBA);¹ and
- the financial institution has not changed its privacy policy and procedures regarding NPI since it sent its most recent GLBA privacy notice to consumers.

This amendment to GLBA was effective immediately, so financial institutions planning to send out annual privacy notices in 2016 may no longer need to do so and may wish to review their privacy practices and procedures to determine if the FAST Act exemption applies. The new FAST Act exemption will not apply to all financial institutions: if, for example, a financial institution changes its practices and discloses NPI to nonaffiliated third parties in a manner that would require it to offer customers an opt-out, the financial institution would be required to send a revised privacy notice to its customers.

In addition to Section 75001 of the FAST Act, financial institutions should consider the potential application of a Consumer Financial Protection Bureau (CFPB) final rule issued in October 2014, which also allows financial institutions that meet certain requirements and limit data sharing to post privacy notices online in place of mailing

The FAST Act provides long-term funding for highway and infrastructure projects and also includes several privacy- and security-related provisions

notices to individuals. Between the FAST Act and the CFPB rule, financial institutions may save considerably on costs associated with mailing annual privacy notices. Additionally, as U.S. Rep. Blaine Luetkemeyer (R-MO), the sponsor of the GLBA amendment, noted, the FAST Act provisions may help consumers by "put[ting] an end to redundant mailings" and "mak[ing] it more likely for people to pay closer attention to mailings they receive from their financial institutions because they would be receiving fewer."

FAST Act Provisions Relating to Transportation and Infrastructure Privacy and Security

In addition to exempting certain financial institutions from annual privacy notice requirements, the FAST Act also includes a number of transportation- and infrastructure-related privacy and cybersecurity matters, including the following:

¹ Specifically, these exceptions are set forth in the following GLBA sections: Sections 502(b)(2) (permitting the disclosure of NPI to a nonaffiliated third party to perform services for or functions on behalf of the financial institution if the financial institution fully discloses the providing of such information and enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information); 502(e) (permitting disclosure of NPI for, inter alia, effectuating or administering transactions for consumers, with the consent of consumers, protecting certain rights of or complying with legal obligations binding upon the financial institution, consumer reporting purposes permitted under the Fair Credit Reporting Act, or in connection with mergers or acquisitions); and 504(b) (permitting primary regulators for financial institutions to promulgate additional exceptions to the GLBA's general bar on NPI disclosure).

Continued on page 11...

FAST Act Eases GLBA Compliance Burdens . . . *(continued from page 10)*

- *Driver Privacy.* Sections 24301–24303 of the FAST Act establish rights to the data stored by event data recorders (e.g., “black boxes”) in vehicles. Under the FAST Act, “[a]ny data retained by an event data recorder . . . is the property of the owner . . . or lessee . . .” of the vehicle. The FAST Act also provides that data stored or transmitted by such devices cannot be accessed by anyone other than the owner or lessee except where: (1) there is a court order; (2) the owner or lessee consents; (3) the data is retrieved pursuant to certain National Transportation Safety Board or Department of Transportation authorized investigations and most personally identifiable information is not disclosed; (4) the data is needed to facilitate emergency medical response to a crash; or (5) the data is to be anonymized and used for traffic safety research purposes. This will likely limit the ability of insurers to make use of vehicular black box data unless the insurer has obtained prior owner/lessee consent. Finally, Section 24303 of the FAST Act also provides for the Administrator of the National Highway Traffic Safety Administration to: (i) report to Congress upon the results of a study conducted to determine the amount of time event data recorders in passenger motor vehicles should

capture and record vehicle-related data in conjunction with an event in order to provide sufficient information to investigate the cause of motor vehicle crashes; and (ii) promulgate related regulations.

- *IoT and Transportation Privacy.* Section 3024 of the FAST Act requires the Secretary of Transportation to issue a report and recommendations on the “Internet of Things to improve transportation services in rural, suburban, and urban areas,” which must address “best practices to protect privacy and security” in connection with transportation and the Internet of Things.
- *Transportation Security Research.* Section 6006 of the Fast Act provides \$400 million in funding for the Department of Transportation to research “Intelligent Transportation Systems,” including research into the development of tools “to help prevent hacking, spoofing, and disruption of connected and automated transportation vehicles.”
- *Electric Infrastructure Cybersecurity.* Section 61003 of the FAST Act implements several reforms aimed at protecting the U.S. energy infrastructure, including: (i) designating the Department

The Fast Act provides funding for transportation research, including the development of tools to help prevent hacking, spoofing, and disruption of connected and automated vehicles

of Energy as responsible for cybersecurity for the energy sector; (ii) creating new classifications for infrastructure-related information and setting rules regarding the sharing of such information; (iii) defining criteria for declaring federal emergencies relating to the energy infrastructure; (iv) establishing an information-sharing regime for federal agencies with authority over energy infrastructure; and (v) establishing liability protections for energy infrastructure entities when sharing information or complying with Department of Energy requests during emergencies, except for actions that are determined to be “grossly negligent.”

EU Agrees to New Cybersecurity and Incident Notification Rules



Sarah Cadiot
Associate, Brussels
scadiot@wsgr.com

The European Union will soon have its own first-ever cybersecurity rules, which will impact a broad range of industries, such as transportation, energy, and online marketplaces. On December 7, 2015, the European Parliament and the Council of the European Union, which is comprised of representatives of the 28 EU countries, reached a political agreement on the draft Directive on Network and Information Security (the NIS Directive).¹ Although the final text is still being finalized at the technical level, it is expected to be formally adopted in early 2016.

Background

In February 2013, the European Commission launched its Cybersecurity Strategy,² which included a proposal for the NIS Directive.³ Like any other EU directive, the NIS Directive will not apply automatically in each EU country once adopted, but will have to be transposed into national legislation by local law. The purpose of the NIS Directive is to harmonize the cybersecurity rules in the various EU countries. However, EU countries will have some leeway when transposing the NIS Directive into national law (e.g., regarding the rules on penalties applicable to infringements of national provisions adopted pursuant to the NIS Directive, as long as such penalties are “effective, proportionate and dissuasive”).

Scope

The scope of the NIS Directive was strongly debated during the legislative process, in particular regarding the types of industries to which the NIS Directive would apply. Ultimately, the NIS Directive applies to many industry sectors, namely to the sectors of energy, transportation, banking, financial market infrastructure, health, drinking water supply and distribution, and digital infrastructure (i.e., Internet exchange points, domain names system services providers, and top-level domain name registries). In addition, it also captures companies providing certain online services.

Below are some examples for the two main categories of industries captured by the NIS Directive:

- “Operators of essential services” (e.g., electricity suppliers, air carriers, credit institutions, trading venues operators, healthcare institutions, water supply and distribution operators)⁴
- “Digital service providers” (i.e., online marketplace operators,⁵ search engine operators, cloud providers) that have their main establishment in the EU or are not established in the EU but are offering digital services within the EU (in which case they must appoint an EU representative), except for the small enterprises (i.e., companies with less than 50 employees and an annual turnover of less than €10 million)⁶

Main Requirements of the NIS Directive

- *Incident Notification Requirement.*
The incident notification requirement is certainly the most important change that the NIS Directive will bring to companies in regard to security, and it goes beyond the existing⁷ or upcoming⁸ EU breach notification requirements pertaining to personal data. The companies captured by the NIS Directive must notify their national regulator about security incidents that have a significant impact on the continuity of their services without undue delay. The regulator will decide whether to inform the public when it is deemed that public awareness is necessary for incident mitigation or prevention purposes.

All concerned companies should take into account specific criteria in determining whether an incident has a significant impact on their services. Those criteria are: (1) the number of users affected by the disruption of the essential service; (2) the duration of the incident; and (3) the geographical area affected by the incident. Moreover, “digital service providers” should take into account the following two additional factors: (1) the extent of the disruption of the functioning of the service; and (2) the impact on economic and societal activities.

For “operators of essential

¹ European Parliament’s press release at <http://www.europarl.europa.eu/news/en/news-room/content/20151207IPR06449/html/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity>.

² Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace, JOIN (2013) 1 (February 7, 2013), <http://ec.europa.eu/digital-agenda/en/news/communication-cybersecurity-strategy-european-union-%E2%80%93-open-safe-and-secure-cyberspace>.

³ Proposal for a Directive concerning measures to ensure a high common level of Network and Information Security across the Union, COM (2013) 48 final (February 7, 2013), <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2013:0048:FIN>.

⁴ The NIS Directive requires each EU country to identify the entities that qualify as “operators of essential services” in its territory; therefore the examples may differ from country to country.

⁵ “Online marketplace” can be practically understood as a web merchant, although the Directive includes a much more complicated definition.

⁶ Online marketplace operators, search engine operators and cloud providers are explicitly qualified as “digital service providers” under the NIS Directive.

⁷ Currently, only a few EU countries require the notification of breaches under data protection law (e.g., Germany, Norway, and the Netherlands), which includes notification to regulators and affected individuals and concerns all business sectors. A few other countries require personal data breaches to be notified only to affected individuals, instead of a regulator, or follow a voluntary notification regime. A sector-specific breach notification requirement exists to date only for EU telecom operators and Internet service providers under the EU e-Privacy Directive 2002/58/EC (amended by Directive 2009/136/EC).

⁸ Although a pan-EU data breach notification for all sectors will be introduced early this year with the planned adoption of the EU General Data Protection Regulation (GDPR), this will only come into effect in two years from now.

Continued on page 13...

EU Agrees to New Cybersecurity . . . (continued from page 12)

services,” regulators will have to adopt guidelines as to how to implement the incident notification requirement. For “digital service providers,” the European Commission will adopt some decisions (so-called “implementing acts”) which will further specify the incident notification requirements at the EU level. Thus, there is some risk of fragmentation of the incident notification requirements in the EU for some parts of the NIS Directive.

- **Mandatory Network Security Measures.** All concerned companies must implement “appropriate and proportionate” technical and organizational measures to manage the risks related to the security of their networks and information systems. The aim is to minimize the potential impact of security breaches and to ensure the continuity of the services. In particular, “digital service providers” must take into account the following when implementing IT risk management solutions: (1) the security of the systems and facilities; (2) an incident management plan; (3) a business continuity plan; (4) monitoring, auditing, and testing programs; and (5) compliance with

international standards.

- **Enforcement Network of Regulators.** Each EU country must designate a national authority for “network and information system security,” by designating existing authorities or creating new ones. The competent authorities must have adequate resources to effectively and efficiently cooperate with each other and to enforce the provisions of the NIS Directive, including the incident notification requirement. The NIS Directive establishes a cooperation mechanism between the national regulators but it remains to be seen how EU countries will effectively cooperate in a timely fashion in cybersecurity cases.

Relation to the GDPR

The political agreement on the NIS Directive is timed closely to the political agreement on the General Data Protection Regulation (GDPR).⁹ Both pieces of EU legislation set out a breach notification requirement but have different scopes and rationale. Since network security incidents (scope of the NIS Directive) are likely to involve personal data (scope of the GDPR), there will be situations where companies must comply with both regimes.

However, the practical implications of such overlap and co-existence are presently unclear. Guidelines by regulators would be useful in this regard.

Next Steps

The timeline for final adoption of the NIS Directive is currently being finalized by EU officials; however the final text is expected to be officially adopted in Spring 2016. Once adopted and effective at the EU level, the new rules would have to pass the green light from national parliaments to become enforceable as part of national legislation. EU countries are directed to implement the NIS Directive into their national law within 21 months after it enters into force at the EU level, thus concerned businesses should already start preparing for the future.

⁹See WSGR Alert, “Political Agreement Reached for New EU Data Protection Regulation—Official Adoption Around the Corner,” December 15, 2015, <https://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-EU-data-protection-1215.htm>.

HHS Ends 2015 with Three HIPAA Enforcement Settlements



Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

In late 2015, the U.S. Department of Health and Human Services (HHS) announced three settlements in which the agency will collect over \$5 million in collective penalties for alleged non-compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). In addition to the monetary penalties, each of the settlements requires compliance with a Corrective Action Plan (CAP), calling for the organizations to invest significant resources toward HIPAA compliance.

Alleged Violations

In all three cases detailed below, HHS began an investigation after it received notice of breaches of unsecured protected health information (PHI). These investigations can take anywhere from a few months to several years to complete. Each organization that was investigated seems to have had some HIPAA-compliance measures in place. However, HHS concluded in all three cases that the organizations did not perform an adequate and thorough data security risk assessment, as required by the HIPAA Security Rule. The agency implied that the data breaches and other alleged gaps in HIPAA compliance stemmed, in part, from this oversight.

HHS investigated Lahey Clinic Hospital after it reported to HHS in 2011 that it had discovered an unencrypted laptop containing the PHI of approximately 600 individuals was stolen from an unlocked treatment room where it was connected to lab equipment.¹ As part of the investigation, HHS alleged several areas of noncompliance with HIPAA, including: the failure to conduct an accurate

and thorough data security risk assessment; the failure to implement physical safeguards of the laptop; the failure to properly track computer inventory movement; the failure to have unique user names for logging into the laptop; the failure to implement a mechanism to monitor activity on the laptop, and the unauthorized disclosure of PHI.

HHS investigated Triple-S Management Corporation and its subsidiaries following seven separate instances of unauthorized PHI disclosures since 2010.² The alleged breaches included former employees accessing PHI after employment termination, using vendors without a business associate agreement (BAA) in place, and mailing PHI to the wrong individuals. HHS alleged that Triple-S did not comply with HIPAA when it: failed to conduct an accurate and thorough data security risk assessment that covered all equipment; failed to implement appropriate data security measures; did not have BAAs in place with vendors; disclosed more PHI than necessary for a particular purpose; failed to terminate access to PHI after an employment termination; and disclosed PHI to unauthorized recipients.

The health affiliates of the University of Washington (UW Medicine) allegedly suffered a breach of PHI in 2013, when an employee downloaded malware through an email attachment.³ The malware allegedly infiltrated UW Medicine's network and compromised approximately 90,000 patient records. HHS investigated the breach and concluded that UW Medicine had failed to conduct an accurate and thorough data security risk assessment.

Corrective Action Plans

In addition to the monetary penalties, HHS required each organization noted above to comply with a CAP and annual reporting

requirements. In all three cases, the CAP requires the organizations to develop a current, comprehensive, and thorough risk analysis of security risks and vulnerabilities within specified deadlines. Triple-S is also required to develop a process for evaluating environmental and operational changes that affect data security. All three organizations then need to submit the risk assessment to HHS for approval. Once their risk assessments are approved, the organizations must send a risk management plan to HHS for approval.

HHS also required Triple-S and Lahey to update their HIPAA-related policies and procedures so that they comply with HIPAA and are adjusted based on the risk management plan. Triple-S is required to annually update the policies and procedures and to submit them to HHS for review and approval for the next three years. The organizations have 30 days to implement the updated policies and procedures following approval by HHS. They are also required to internally distribute and provide employee training on the updated policies and procedures. In addition, Triple-S is required to have its business associates agree to abide by such policies and procedures.

The organizations have ongoing obligations for the length of their CAP two years for UW Medicine and Lahey, and three years for Triple-S. During this time, they are required to notify HHS of any workforce violations of their HIPAA-related policies and procedures, even when they do not result in a breach of PHI. UW Medicine and Triple-S also must submit annual compliance reports.

Implications

With HIPAA audits likely coming in 2016,⁴ these enforcement actions may provide valuable insight into HHS's plans for such

¹See the Resolution Agreement with Lahey at <http://www.hhs.gov/sites/default/files/lahey.pdf>.

²See the Resolution Agreement with Triple-S at <http://www.hhs.gov/sites/default/files/Triple-S%20-%20OCR%20Resolution%20Agreement%20and%20Corrective%20Action%20Plan%20in%20Final%20%28508%29.pdf>.

³See the Resolution Agreement with UW Medicine at <http://www.hhs.gov/sites/default/files/uw-ra-and-cap.pdf>.

⁴See *The WSGR Data Advisor*, "No More Crying Wolf—HIPAA Audits Coming in 2016," November 2015, <https://www.wsgr.com/publications/PDFSearch/the-data-advisor/Nov2015/#8>.

Continued on page 15...

HHS Ends 2015 with Three HIPAA Enforcement . . . *(continued from page 14)*

audits. It is no secret that the 2012 audits identified a frequent lack of compliance with HIPAA's requirements that entities perform annual data security risk assessments and implement risk management plans to mitigate any identified security risks and vulnerabilities. These recent enforcement actions show that this area continues to be a weakness in organizations' compliance efforts. Organizations chosen for a random audit should be prepared to provide their

risk assessments and management plans to HHS. Now is a good time for organizations to ensure their risk assessments and management plans are current, comprehensive, and thorough.

The settlements also indicate that HHS may take an active role in ensuring an organization's HIPAA compliance. In these cases, HHS was not satisfied solely with imposing a monetary penalty when an

organization allegedly violates HIPAA; it also requires a detailed CAP where it sets an aggressive timeline for an organization to fix the alleged problems with the organization's HIPAA compliance. The agency also insists that it review and approve an organization's efforts to remediate the alleged problems. Therefore, a settlement with HHS may lead to two to three years of active involvement in an organization's internal business operations.

Upcoming Industry Events Featuring WSGR Privacy & Data Protection Professionals

Association of Corporate Counsel (ACC) Austin Chapter

"Privacy and Data Security Concerns in a Changing Regulatory Environment"

February 18, 2016

Austin, Texas

- WSGR partner Lydia Parnes and associate Wendell Bartnick will speak on what companies should be doing now to comply with the complex and changing government regulations and industry standards focused on the collection and protection of consumer and employee information.

International Association of Privacy Professionals (IAPP)

Global Privacy Summit

April 3-6, 2016

Washington, D.C.

- WSGR partner Lydia Parnes will speak at the annual conference for international privacy and data protection professionals. More details will be announced soon.

American Bar Association (ABA) Business Law Section Spring Meeting

"Cybersecurity Due Diligence in M&A Transactions"

April 8, 2016

Montreal, QC, Canada

- WSGR associates Jonathan Adams and Matthew Staples will speak on a panel exploring ways in which the ABA's forthcoming Best Practices Guide to Cybersecurity Due Diligence in M&A Transactions might help acquirer and target company boards of directors to better understand and address cyber risks to proposed transactions.

Wilson Sonsini Goodrich & Rosati has a global network of experienced privacy attorneys with whom we have worked extensively. We can assist you with privacy issues in any country, interfacing with local counsel and coordinating the project on your behalf.



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

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

This communication is provided for your information only and is not intended to constitute professional advice as to any particular situation.
© 2016 Wilson Sonsini Goodrich & Rosati, Professional Corporation. All rights reserved.

