Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

THE WSGR DATA ADVISOR

NOVEMBER 2015

Welcome

The last two months certainly have been eventful in the world of privacy. In this issue of *The WSGR Data Advisor*, we examine the Court of Justice of the European Union's recent and highly significant *Schrems* decision that invalidated the U.S.-EU Safe Harbor framework. We also present the third article in our series discussing the importance of data considerations in the transactional context with a look at privacy and data security due diligence. And, we explore two recent settlements with the California Attorney General, including the largest privacy settlement on record.

From the regulatory side, we provide a recap of the FTC's first "Start with Security" conference, we discuss recent data security guidance from the SEC, we detail guidance from The PCI Security Standards Counsel on responding to a data breach, and we examine the permanent HIPPA privacy and security audit program, which will be launched in early 2016. Finally, we discuss another landmark decision in the EU addressing the territorial scope of application of national data protection laws.

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 & Michael Rubin
Wilson Sonsini Goodrich & Rosati

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

Michael Rubin
Partner, San Francisco
mrubin@wsgr.com

What's Next for U.S.-EU Data Transfers? An Analysis of Recent Developments Following *Schrems*

Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com

Sarah Cadiot
Associate, Brussels
scadiot@wsgr.com

Laura De Boel
Associate, Brussels
ldeboel@wsgr.com

On October 6, 2015, the Court of Justice of the European Union (CJEU) invalidated the U.S.-EU Safe Harbor framework as a legal basis for transferring personal data from the European Union to the U.S.[1] The judgment was delivered in *Schrems v. Data Protection Commissioner*, a case in which Max Schrems, an Austrian student, complained to the Data Protection Authority (DPA) in Ireland about the transfer of his personal data by Facebook to its servers in the U.S.

The *Schrems* judgment is of major importance to the over 4,000 companies that relied on Safe Harbor to transfer personal data from the EU to the U.S. This article details the background of the case, analyzes its holdings and consequences, and summarizes the main developments that have occurred since the judgment was issued.

[1] The judgment in case C-362/14 at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=402443.

Background

EU personal data can be transferred outside of the EU only if the laws of the recipient country are deemed to provide an adequate level of data protection under EU law, or if there is a legal mechanism in place to ensure such an adequate level of protection. The European Commission—the EU's executive arm—can adopt "adequacy decisions" to officially approve a country's adequate level of data protection.

In This Issue

EU-U.S. Data Transfers: Safe Harbor Declared Invalid . . . *(continued from page 1)*

The U.S. is not considered to provide an adequate level of data protection under EU law. However, the EU and the U.S. had agreed on a Safe Harbor framework to allow U.S. companies to transfer EU personal data to the U.S. In 2000, the European Commission formally recognized the Safe Harbor framework as a valid mechanism for transferring personal data from the EU to the U.S by adopting an adequacy decision (Safe Harbor decision).[2] By self-certifying to the Safe Harbor framework, companies voluntarily committed to abide by a set of data protection principles. The Safe Harbor framework was enforced by the Federal Trade Commission (FTC) under Section 5 of the FTC Act.

In the wake of revelations concerning mass surveillance by U.S. authorities in 2013, Max Schrems filed a complaint with the DPA in Ireland, where Facebook's EU headquarters is located. Schrems requested that the DPA investigate Facebook's alleged disclosure of EU personal data to U.S. authorities for mass surveillance purposes. The Irish DPA rejected the complaint, arguing that it was bound by the Safe Harbor decision. Schrems appealed to the Irish High Court, which requested that the CJEU clarify whether national DPAs are bound by such adequacy finding by the European Commission.

The Judgment

Below are the key findings of the *Schrems* judgment.

1. *Safe Harbor Is Invalid.* The CJEU went beyond the initial question brought by the Irish High Court and declared the Safe Harbor decision invalid. According to the CJEU, the Safe Harbor decision violated EU fundamental rights due to broad exceptions for data disclosures for national security purposes, the lack of judicial redress for EU individuals in the U.S., and the lack of oversight powers by independent authorities.
2. *Any Further Transfer of Personal Data on the Basis of Safe Harbor Is Unlawful.* As a result of the invalidation of the Safe Harbor decision, any new data transfer by companies that were relying on the Safe Harbor framework now lacks a legal basis and may expose these companies to liability until they implement an alternative data transfer mechanism.
3. *DPAs Can Investigate Data Transfers Based on Adequacy Decisions.* Even if data transfers are occurring on the basis of a European Commission's adequacy decision, each national DPA can independently investigate the transfers (e.g., following a complaint) and decide to suspend them if it considers they violate EU data protection law. This entails a high risk of inconsistent decisions of the different national DPAs concerning international data transfers, and may lead to the fragmentation of the EU internal market, which creates significant uncertainty for businesses.
4. *Alternative Data Transfer Solutions Are Valid for Now.* The judgment did not consider the validity of other data transfer mechanisms, such as Standard Contractual Clauses (SCC), Binding Corporate Rules (BCRs), *ad-hoc* contracts, and derogations such as consent or the performance of a contract. Therefore, for the time being, these mechanisms can still serve as an alternative to the Safe Harbor framework. However, some regulators consider that these alternative data transfer mechanisms should also be investigated (see below).

Stakeholder Reactions

The *Schrems* judgment created a high level of legal uncertainty in the EU, which was increased by various statements from stakeholders in and outside the EU that followed on the judgment. Summarized below are some of the main developments since the release of the judgment.

The European Commission's Statements

On the day of the release of the judgement, the European Commission stated during a press conference that other data transfer mechanisms are available to businesses, and underlined that both the EU and the U.S. are actively engaged in negotiations for a new Safe Harbor framework.[3] A month after the judgment, the European Commission released a non-binding guidance communication on the transfer of personal data from the EU to the U.S. following the *Schrems* judgment. This is a political document which, although being informative, is of little help for businesses.[4]

The Article 29 Working Party's Reaction and Statements from Local DPAs

On October 16, 2015, the Article 29 Working Party (the Working Party)—the body where national DPAs meet at the EU level—issued its first statement on the implementation of the judgement.[5] Statements and guidance from the Working Party are usually a good indication of how DPAs will interpret the law but are not legally binding.

In a nutshell, the Working Party confirmed that: (i) transfers of personal data formerly based on the Safe Harbor framework are now unlawful; and (ii) SCC and BCRs are still valid alternative data transfer solutions. However, the Working Party declared that it will assess the validity of these alternative data transfer mechanisms in light of the *Schrems* judgment and reserve the right to suggest changes to these instruments. In addition, the Working Party urged the European Commission to make progress on enabling data transfers to the U.S. by the end of January 2016, including by negotiating a new agreement with the U.S. This deadline is more an ultimatum given to the EU institutions and U.S. government to find

[2] The European Commission Decision of July 26, 2000 (2000/520/EC) at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.
[3] The European Commission's press release at http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm.
[4] The Communication at http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.
[5] The Working Party's Statement at http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf.

Continued on page 3...

a political solution than a grace period given to companies. DPAs threaten to start coordinated enforcement actions if no solution is found with the U.S. before this date. In the meantime, individual DPAs may already investigate particular cases and exercise their powers, including the suspension of data transfers, in particular in case of complaints from individuals.

In parallel, many DPAs have expressed their own views, which are often not entirely aligned with the Working Party's statement. For example, the German DPAs jointly stated that they would not approve any new BCRs and "data export contracts."[6] Within Germany, each DPA acts independently, and some of them have expressed even more conservative approaches (e.g., the Schleswig Holstein DPA). On the other end of the spectrum, the UK DPA,[7] traditionally quite pragmatic, recommended that companies not rush into alternative solutions. Statements from the Spanish,[8] French,[9] Belgian,[10] Polish,[11] and Italian[12] DPAs can be situated somewhere in between these two ends of the spectrum. Some DPAs, such as the Spanish and Norwegian DPAs, started sending letters to companies that indicated in their registrations Safe Harbor as the legal basis for data transfers to the U.S. Businesses are now facing a high risk of fragmentation of the EU market if DPAs do not fully coordinate their actions. Hopefully, the Working Party will soon issue its own guidance document on the consequences of *Schrems*.

Consequences of the Judgment Outside the EU

The invalidation of the Safe Harbor decision also had an effect outside of the EU. A number of non-EU countries have adopted data protection legislation that is inspired by EU data protection law over the years. Many of these countries consider that countries or mechanisms that are recognized to be adequate under EU data protection law are also adequate under their own national data protection law. Therefore, the invalidation of the Safe Harbor decision also triggered some reactions outside of the EU. In particular, the Swiss[13] and Israeli[14] DPAs considered that data transfers based on the Safe Harbor framework are no longer lawful. In a milder approach, the Dubai International Financial Centre's DPA stated that it is reconsidering the adequacy status granted to Safe Harbor-certified companies.[15]

Companies transferring personal data outside the EU now face a very high level of uncertainty

A New Framework for Data Transfers Between the EU and the U.S.?

The European Commission officially aims to conclude the negotiations on a new agreement before the end of January 2016. Both the U.S. and the EU have made statements that the negotiations are progressing quickly, and that they are hopeful that an agreement will be reached shortly.[16] However, it is uncertain whether the U.S. and the EU can agree on a new framework that will actually meet the very high bar set by the *Schrems* judgment. In particular, there are concerns in the EU regarding the restrictions that should apply to requests for data access by U.S. law enforcement and national security agencies and the possibility for individuals to seek redress in the EU.

Conclusions: Companies Should Monitor the Situation and Consider Implementing an Alternative Data Transfer Strategy

Companies transferring personal data outside the EU now face a very high level of uncertainty regarding the legal framework applicable to their data transfers, and there is a significant risk of fragmentation of the EU internal market. It seems likely that DPAs will take enforcement actions across the EU against companies that have not implemented an alternative data transfer mechanism by the end of January, or before then in case they receive complaints from individuals. In parallel, negotiations between the U.S. and the EU to agree on a new framework are progressing, but it remains uncertain whether a workable agreement will be reached in the short term.

Therefore, companies that were relying on the Safe Harbor framework should adopt a new data transfer strategy. There is no one-size-fits-all alternative approach to Safe Harbor. Which data transfer mechanism to implement depends on a company's size, corporate structure, industry sector, data flows, and whether it operates in the B2C or B2B context.

The situation is in flux and evolving at a fast pace since all stakeholders involved, in and outside the EU, are still figuring out the consequences of the *Schrems* judgment. New developments on this issue are expected in the coming weeks and months. We are closely monitoring this issue and will continue to update you on significant developments.

[6] The position paper (in German) at https://www.datenschutz.hessen.de/ft-europa.htm#entry4521.
[7] The UK DPA's blog post at https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed/.
[8] The Spanish DPA's statement (in Spanish) at http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_06-ides-idphp.php.
[9] The French DPA's statement (in French) at http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/.
[10] The Belgian DPA's statement (in French) at https://www.privacycommission.be/fr/news/la-commission-vie-privee-se-prononce-sur-larret-de-la-cour-de-justice-de-lunion-europeenne.
[11] The Polish DPA's statement (in Polish) at http://www.giodo.gov.pl/560/id_art/8951/j/pl/.
[12] The Italian DPA's statement (in Italian) at http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4308245.
[13] The Swiss DPA's statement (in French) at http://www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr.
[14] The article at https://iapp.org/news/a/safe-harbor-fallout-israels-dpa-revokes-prior-authorization/.
[15] The DIFC DPA's guidance at http://www.difc.ae/sites/default/files/DIFC-Data-Protection-Commissioner-Guidance-on-Adequacy-Status-relating-to-US-Safe-Harbor-Recipients.pdf.
[16] The European Commission's press release at http://europa.eu/rapid/press-release_IP-15-6015_en.htm.

Continued on page 4...

Privacy and Data Security Due Diligence

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

Jonathan Adams
Associate, San Francisco
jadams@wsgr.com

This article is the third in a series of articles that discuss the importance of privacy and data security considerations in the transactional context.

In any transaction in which an entity invests in or acquires another business or its assets, the investing or acquiring entity (the "Acquiror") should fully evaluate its counterparty (the "Company"), the Company's assets, and the Company's liabilities and risks prior to the consummation of the transaction. A spate of significant data security incidents and exposés in the past few years has raised awareness across industries of the need to adequately contemplate privacy concerns and appropriately secure data systems. Businesses, acquirors, and investors increasingly understand that expensive data security incidents, lawsuits, and government investigations can result from basic failures to comply with applicable privacy laws or data processing contracts or, with regard to information security, well-established industry best practices.

Because of the high costs of responding to and managing investigations, litigation, and data security breaches—and the potential disruptions to business and the brand damage that follows—businesses have become increasingly attuned to the need for minimizing risks *before* an incident occurs. Thus, when an Acquiror is evaluating an acquisition, proper risk management requires the Acquiror to take the time and to expend the resources necessary to conduct targeted due diligence, and to mitigate and manage data privacy and security-related risks. When a Company fails to appropriately handle privacy or data security matters, and those matters are not identified and addressed prior to consummating a transaction, undesirable or even disastrous results could follow. For instance, if an Acquiror has not appropriately allocated risks for privacy or data security compliance to the Company, the Acquiror could end up losing a significant portion of the deal value.

Failure to appropriately evaluate privacy or data security considerations in a merger or acquisition could result in an Acquiror: (a) purchasing data or data systems that cannot be appropriately or meaningfully used or exploited; (b) acquiring compromised electronic assets or data systems; (c) inheriting class actions or governmental investigations or fines; or (d) experiencing losses in value or brand equity following a deal. If a Company fails to adequately manage its privacy or data security risks, the Acquiror may also face significant market risk with respect to the acquired business. In one well-publicized example, Target Corporation suffered a significant data breach that it announced on December 19, 2013. In the ensuing two months, Target's stock lost more than ten percent of its value.[1] Fixing these privacy and data security problems can become very costly—for instance, Home Depot announced in September 2014 that it anticipated spending about $62 million to handle the investigation, credit monitoring services, call center staffing, and other remediation-oriented steps to respond to the breach of 56 million payment cards compromised in a massive cyber attack.[2] These financial repercussions have lasting effects on a company's financials and, perhaps more importantly, on a company's brand, with many consumers choosing to avoid conducting business with brands that they consider to have exposed consumers' personal information.[3]

In certain cases, a failure to appropriately evaluate these risks could lead to an Acquiror's unwillingness to consummate an agreed-upon transaction because of the potential costs and risks, or because of the difficulties in integrating a business or its assets.[4] Indemnification may be available in certain circumstances, but difficulties may arise in obtaining indemnification, and indemnification may be subject to caps or other limitations that prevent an Acquiror from being made whole for its losses. When one adds to this the potential risks of data security incidents occurring during the process of negotiating or consummating a transaction—i.e., the potential that one or more parties to a potential strategic transaction is targeted by hackers or others who use information transfers and sharing in connection with the proposed transaction in order to advance an agenda, such as espionage or gaining a competitive advantage—the importance of considering the potential privacy and data security risks to Acquirors in the course of effectuating a transaction becomes paramount.[5]

---

[1] *See* Andria Cheng, "Two Months After Damaging Data Breach, Target Stock Has Its Best Day in Five Years," MarketWatch, February 26, 2014, http://blogs.marketwatch.com/behindthestorefront/2014/02/26/two-months-after-damaging-data-breach-target-stock-has-its-best-day-in-5-years/. *See also* "Home Depot: Could the Impact of the Data Breach Be Significant?" Forbes Great Speculations Blog, September 24, 2014, http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/.

[2] *See id.*

[3] Mark Bribish, "A Data Breach Will Damage Your Business, Brand, and Profits—Are You Prepared?" *The Arizona Republic*, July 17, 2014, http://www.azcentral.com/story/money/business/2014/07/17/data-breach-will-damage-business-brand-profits-prepared/12805227/.

[4] *See* Dale S. Bergman, "Notable Factors and Trends in Recent M&A Deals," *M&A Deal Strategies*, September 2012, at 7 ("Ultimately, when an M&A deal fails, it is often because the buyer did not do its diligence. An acquirer needs to know exactly what it is buying, what liabilities it is assuming, and how the acquisition is going to affect the acquirer from a financial and operational point of view.").

[5] This is far from an academic concern: in the past decade, numerous deals have been targeted by hackers affiliated with interested parties or competitors. *See, e.g.*, Michael A. Riley and Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data," Bloomberg, January 31, 2012, http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html.

Continued on page 5...

Privacy and Data Security Due Diligence . . . *(continued from page 4)*

Acquirors must consider myriad privacy and data security matters in mergers, acquisitions, and other strategic transactions. Through conducting due diligence, Acquirors may discover risks related to inadequate privacy or data security programs and procedures, litigation risks, undisclosed data breaches, government investigations, non-compliance with legal or industry obligations, or other similar matters related to the Company's management of personal data and assets. Lawyers focused on privacy and data security issues can ensure that these risks are evaluated, disclosed, and remediated appropriately. The Acquiror's counsel should work with the Acquiror's business and technical subject matter experts to determine whether steps need to be taken by the Acquiror or the Company to enable the Acquiror to use any personal data and other information assets that are transferred in a transaction. Acquirors should also attempt to ensure that representations and warranties addressing privacy and data security are drafted, structured, and negotiated effectively to cause risk (and costs) to be allocated to the Company and its owners.[6] Further, in order to effectuate a contemplated transaction, Acquirors must consider how to address data transfer issues. In some cases, an Acquiror may need to ensure that clauses regarding data transfer rights, user or employee consents, the security of transferred data and assets, and other critical matters are tailored appropriately, and to make sure that appropriate steps are taken by the Company to transfer such data and assets and to permit their contemplated use by the Acquiror.

In mergers and acquisitions, parties conduct due diligence to understand the nature of the facts that relate to, and the risks that may arise from, the proposed transaction and the acquired entity and business. In these transactions, due diligence is typically performed so that an Acquiror can learn more about the Company or the Company's assets that are being acquired and how the Company or its assets may be integrated into the Acquiror's business. In these circumstances, conducting due diligence may include discussing the Company's business with key employees; reviewing relevant policies, procedures, documentation, and contracts; reviewing litigation and pre-litigation activity; and identifying other commitments. The findings from due diligence may shape the structure of a transaction, may necessitate additional representations, warranties, or covenants of the Company, and may materially affect the consideration received by the Company and its owners in connection with a transaction.

More specifically, privacy and data security due diligence provides an opportunity for the relevant parties in a transaction to learn about and evaluate the Company's data privacy, data security and information governance policies and practices. There are many avenues that produce relevant information in the course of privacy and data security due diligence. To begin with, a Company's public statements—in the Company's website privacy policies, public securities filings, press releases, product claims, employee quotes, and other public-facing documents—can be remarkably useful in understanding how the Company views or characterizes itself and presents itself to consumers, investors, and the general public. These public statements should not, however, be taken at face value, and this review is only the first component of privacy and data security due diligence.

The information that an Acquiror should attempt to gather through due diligence in an acquisition or financing can vary dramatically across companies and industries and should be based on the probable risks associated with a Company. Companies that operate in regulated sectors—such as financial services, healthcare, critical infrastructure, and transportation—can present more significant risks to an Acquiror, and thus Acquirors should ask more probing and target-appropriate questions when conducting due diligence upon such Companies. Similarly, larger or more complex Companies may pose additional due diligence hurdles based upon the sheer volume of materials that must be reviewed in the short window of time prior to entering into the transaction documents. In any such transaction, the Acquiror should ensure that it allocates the appropriate time and resources to diligence matters in order to fully understand the more complex risk patterns endemic in transactions involving large Companies.

The findings in privacy and data security due diligence can have a significant effect on a transaction: by better knowing a Company and its data practices, an Acquiror can more easily evaluate the company's potential risks. Due diligence may reveal non-compliance with laws or with contractual requirements, or might uncover that a Company has experienced significant data security vulnerabilities, including data breaches, or that a Company is restricted from transferring data to the Acquiror and permitting its use by the Acquiror.[7]

---

[6] The structure of a strategic transaction may affect the data rights of the Acquiror, and may result in additional risks being borne by the Acquiror, too. For instance, in mergers or stock purchases, an Acquiror may be assuming the Company's past liabilities for privacy and data security compliance issues, including regulatory investigations and litigation. At the same time, certain concerns regarding whether data may be "transferred" in a strategic transaction are not as relevant in mergers or stock purchases in which the Company continues operations. In conducting due diligence upon a Company, Acquiror's counsel should keep in mind the structure of the strategic transaction to appropriately evaluate the Company's risks.

[7] The FTC and state authorities have intervened to preclude the transfer of certain personal data in mergers, acquisitions, and bankruptcies where the privacy policy of the company attempting to transfer personal data did not permit the transfer of personal data in such transactions. *See, e.g., FTC v. Toysmart.com, LLC, and Toysmart.com, Inc.*, No. 00-11341-RGS (Stipulated Consent Agreement and Final Order) (D. Mass. July 21, 2000); Letter from David C. Vladeck, Director, Bureau of Consumer Protection, Federal Trade Commission to XY Magazine and XY.com Regarding the Use, Sale, or Transfer of Personal Information Obtained During Bankruptcy Proceeding, July 1, 2010, http://www.ftc.gov/system/files/documents/closing_letters/letter-xy-magazine-xy.com-regarding-use-sale-or-transfer-personal-information-obtained-during-bankruptcy-proceeding/100712xy.pdf; Letter From Jessica L. Rich, Director of the Federal Trade Commission Bureau of Consumer Protection, to Erin Egan, Chief Privacy Officer, Facebook, and to Anne Hoge, General Counsel, WhatsApp Inc., April 10, 2014, http://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf; *In the Matter of State of Texas and True Beginnings d/b/a True.com*, No. 12-42061, Assurance of Voluntary Compliance (Tex. Dist. Ct. of Travis County, November 14. 2013).

Continued on page 6...

Privacy and Data Security Due Diligence . . . *(continued from page 5)*

An Acquiror can then use its due diligence findings to more appropriately allocate risk for privacy or data security matters to the Company. For example, the Acquiror could use due diligence findings to ensure that indemnification provisions and other remedies that may be available to the Acquiror, and attendant limitations upon them, are adequate in light of potential risks. Likewise, an Acquiror can determine whether certain privacy and data security risks need remediation prior to signing or closing, or whether the risks can be handled by the Acquiror post-closing. If risks are particularly significant, an Acquiror may find it prudent to seek additional assurances from the Company or may modify the pricing for a particular transaction or, in some cases, may elect not to proceed with the transaction. Without conducting appropriate due diligence, however, addressing the Company's privacy or data security practices may be difficult.

Comcast Enters into Largest Privacy Settlement on Record with California Attorney General

Christopher Olsen
Partner, Washington, D.C.
colsen@wsgr.com

On September 17, 2015, California Attorney General Kamala Harris announced a $33 million settlement with Comcast Corp. to resolve an investigation into Comcast's publishing of phone numbers that consumers had paid the company not to publish.[1] Notably, the settlement is the largest privacy settlement on record to date, surpassing the recent $25 million settlement the Federal Communications Commission (FCC) obtained from AT&T in April 2015.[2] The action is also notable for which agency brought it and which agencies did not participate—this was a California state action and not an FCC or Federal Trade Commission (FTC) enforcement proceeding. The FTC has been the leading privacy enforcer over the last twenty years, and the FCC has spent the last two years nipping at the FTC's heels on privacy enforcement. So, why did the two leading federal privacy regulators apparently sit on the sidelines for the largest privacy settlement on record? This article examines that question and posits some theories on why the other agencies may not have proceeded. Regardless of whether federal regulators decided to act in this case, the Comcast settlement with California offers a stark reminder for companies that failing to protect consumer privacy or misleading consumers about privacy protections can land you in expensive hot water on a wide variety of regulatory fronts.

California's Settlement with Comcast

The complaint filed by California against Comcast lays out a fairly straightforward set of facts. Comcast provides Voice over Internet Protocol (VoIP) service to California residents.[3] Beginning in July 2010, Comcast began publishing online directory listings (i.e., name, address, phone number) and licensing its listings to a third party for publication and directory assistance. Comcast offered customers the option to have their numbers non-listed (for $1.25 a month) or non-published (for $1.50 a month). Because of some internal account management changes, Comcast failed to flag the non-published status of requesting customers when Comcast transmitted the records to its third-party vendor for directory publishing. As a result, from around July 2010 to December 2012, approximately 75,000 consumers who had requested non-listed or non-published status had their phone numbers published in directory listings and made available by directory assistance providers.

According to the complaint, Comcast received consumer complaints about the publishing of non-published and non-listed numbers, and in December 2012, Comcast deleted the numbers from its directory listings. Comcast also informed affected consumers that their information had been made public. A number of customers, including law enforcement officials, judges, domestic violence victims, and other crime victims raised safety concerns related to the publishing of their directory listing information.

California filed its complaint and stipulated final judgment on September 17, 2015, in California state court. Pursuant to the terms of the stipulated final judgment, Comcast was required to pay $7,909,400 in restitution to affected customers and $25 million in penalties, including $12.5 million to the California General Fund, and $12.5 million to the California attorney general's office.[4] In addition to the significant monetary payments, the stipulated final judgment imposed a number of substantial injunctive requirements.

Why Was This Not an FCC Case?

There are a number of reasons why one could rightly ask why the Comcast incident was not the subject of an FCC enforcement

[1] Press Release, California Attorney General, "Attorney General Kamala D. Harris Reaches $33 Million Settlement with Comcast over Privacy Violations," September 17, 2015, https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-reaches-33-million-settlement-comcast-over.

[2] *See* Order & Consent Decree, AT&T Services, Inc., File No. EB-TCD-14-00016243 (FCC April 8, 2015), https://transition.fcc.gov/eb/Orders/2015/DA-15-399A1.html.

[3] Complaint, *California v. Comcast*, No. RG15789197 (Cal. Super. Ct. Alameda Cnty. September 17, 2015), https://oag.ca.gov/system/files/attachments/press_releases/People%20of%20CA%20v%20Comcast%20complaint%20RG15786197%20Alameda%20Superior.pdf?

[4] Final Judgment and Permanent Injunction, California v. Comcast, No. RG15789197 (Cal. Super. Ct. Alameda Cnty. September 17, 2015), https://oag.ca.gov/system/files/attachments/press_releases/Comcast%20final%20judgment%20and%20permanent%20injunction.pdf? (hereinafter Final Judgment).

Continued on page 7...

Comcast Enters into Largest Privacy Settlement . . . *(continued from page 6)*

action. First, the incident involved information protected by a core provision of the Communications Act enforced by the FCC—Section 222, Privacy of Customer Information. Second, it involved a cable provider obligated to protect the privacy of the information in question under the Cable Communications Policy Act, which the FCC also enforces.[5] Finally, the FCC has been very active on the privacy enforcement front since Travis LeBlanc assumed the reigns of the Enforcement Bureau in early 2014. In addition to a $25 million settlement with AT&T for Section 222 privacy violations, LeBlanc also obtained a $7.4 million settlement with Verizon and a $3.5 million settlement with TerraCom and YourTel for similar violations. He has publicly declared that privacy enforcement is a top priority for the agency.[6] Finally, immediately prior to joining the FCC, LeBlanc worked as a senior advisor to California Attorney General Kamala Harris; it would not be surprising to learn that he and the attorney general compared notes on Comcast's privacy troubles.

So why did the FCC not pursue Comcast or join California's action against Comcast? One likely reason has to do with a significant limitation built into the portion of the Communications Act authorizing the FCC to take action for violations. Section 503(b)(6) of the act states, "[n]o forfeiture penalty shall be determined or imposed against any person under this subsection if . . . the violation charged occurred more than [one] year prior to the date of issuance of the required . . . notice of apparent liability." According to the complaint California filed against Comcast, the company ceased engaging in the problematic conduct in December 2012. Thus, the FCC would have had to issue a Notice of Apparent Liability[7] by December 2013 to pursue a forfeiture under its statutory authority, and the FCC did not act within that timeframe. That timing was likely fortuitous for Comcast, as its exposure to a forfeiture here would have been quite substantial: $37,500 per violation times 75,000 violations for a maximum forfeiture of close to $3 billion.[8]

Even in instances like this where the conduct is beyond the reach of the FCC's forfeiture authority, companies should remain mindful that they are not out of the woods for violations of the Communications Act. Under Sections 206-209 of the act, individuals can file complaints with the FCC or in district court for violations of the Communications Act, and the FCC and courts are authorized to award damages in such cases.[9] Further, the statute of limitations under Section 503(b)(6) of the Communications Act does not apply to complaints brought under these sections of the act. Finally, for violations of the Cable Communications Policy Act, consumers are authorized to file suit in federal district court seeking actual damages, punitive damages, and reasonable attorney's fees and litigation costs.[10]

Why Was This Not an FTC Case?

The FTC has been bringing privacy cases since the late 1990's,[11] and is widely regarded as the leading privacy enforcer in the United States.[12] The lead count in California's complaint against Comcast is that Comcast misled its customers regarding the privacy of their information—a count that closely resembles counts in many FTC complaints alleging deceptive conduct in violation of Section 5 of the FTC Act. So why was the FTC not in on the action here? The FTC, unlike the FCC, does not have a one-year statute of limitations, so that cannot be the reason for the apparent reticence to act.

One potential explanation for FTC caution may have to do with the common carrier exemption in the FTC Act. The FTC is authorized under Section 5 "to prevent persons, partnerships, or corporations, except . . . common carriers subject to the Acts to regulate commerce . . . from using . . . unfair or deceptive acts or practices in or affecting commerce." The "Acts to regulate commerce" in the FTC Act include the Communications Act enforced by the FCC. The cause of action here involved telephone service so the FTC would likely have had to consider jurisdictional issues in deciding whether to look into Comcast's behavior. And, while the FCC has not declared the precise service at issue, interconnected VoIP, to be a common carrier service under the Communications Act, the FCC has subjected

---

[5] Indeed, California's complaint cites the violation of the Cable Communications Policy Act as a basis for its cause of action alleging a violation of the California's Unfair Competition law.

[6] Mike Swift, "Privacy Will Be A Key Enforcement Issue For FCC under Open Internet Rules, Enforcement Chief Says," MLEX, March 13, 2015, http://mlexmarketinsight.com/landing-pages/privacy-will-be-a-key-enforcement-issue-for-fcc-under-open-internet-rules-enforcement-chief-says/; Brandon Ross, "FCC Enforcement Chief Outlines New Focus: Consumers, Prevention, Efficiency," BNA.COM, July 23, 2014, http://www.bna.com/fcc-enforcement-chief-n17179892750/.

[7] A Notice of Apparent Liability (NAL) is the first step that the FCC must take to order a commission licensee to pay a forfeiture. In an NAL, the FCC concludes that a company is "apparently" liable for violations of the Communications Act and or commission rules and that it should pay a forfeiture of a specified amount. The recipient of the NAL has an opportunity to respond, challenging the factual basis of the NAL, the legal conclusions stated in the NAL, and the proposed forfeiture amount. The commission then determines whether to proceed with a forfeiture order.

[8] Of course, it is very unlikely that the FCC would propose a forfeiture this significant. It would, however, use this maximum exposure amount to justify a very high proposed forfeiture amount or required settlement payment. In its NAL against TerraCom and YourTel, for example, the FCC arrived at a proposed forfeiture amount of $10 million after noting that the potential exposure of the companies for privacy violations was close to $9 billion under the statutory forfeiture provisions. *See* Notice of Apparent Liability for Forfeiture, TerraCom, Inc. and YourTel America, Inc., File No. EB-TCD-13-00009175, at ¶ 52 (FCC October 24, 2014), https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-173A1.pdf

[9] These provisions of the Communications Act apply only to common carrier violations of the act. As noted *infra*, the FCC has not declared interconnected VoIP providers to be common carriers. The FCC, has, however, required interconnected VoIP providers to meet basic common carrier obligations of the Communications Act and has invited consumers to submit complaints against VoIP providers for violations of those provisions. Thus, it seems likely that the FCC would subject interconnected VoIP providers to the complaint provisions in the act.

[10] 47 U.S.C. § 551(f).

[11] *See* Press Release, FTC, "Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case," August 13, 1998, https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting.

[12] *See, e.g.*, Brendan Sasso, "FTC Steps In As Obama's Chief Enforcer on Internet Privacy," *The Hill*, May 13, 2012, http://thehill.com/policy/technology/227037-ftc-steps-in-as-obamas-chief-enforcer-on-internet-privacy; Stephen Cobb, "America's Privacy and Security Enforcer," SCMagazine.com, July 6, 2012, http://www.scmagazine.com/americas-privacy-and-security-enforcer/article/249082/2/.

Continued on page 8...

Comcast Enters into Largest Privacy Settlement . . . *(continued from page 7)*

interconnected VoIP to several core common carrier-related provisions of the act, including the requirements related to consumer privacy.[13] Thus, the FTC might have faced a challenge by Comcast to any attempt to pursue enforcement action in this case. Comcast might have argued that the FCC's regulation of the precise service at issue under common carrier provisions of the Communications Act renders the activity exempt from FTC oversight under Section 5 of the FTC Act. The FTC, to the extent the Comcast incident was ever on its radar screen, may have concluded that the jurisdictional fight was not worth having.

In this case, it is hard to know whether the FTC ever looked at Comcast's practices, and, if so, what the FTC considered in determining whether and how to proceed. At this point, though, after California's significant action against Comcast, it seems unlikely that the FTC would get involved. The FTC would likely conclude that its limited resources are best directed to other potential targets that have not already been the subject of major regulatory action.

Conclusion

Privacy enforcement actions used to be the sole province of the FTC. This is no longer the case. The FCC has become very active in this space in the past two years. More and more, state attorneys general are getting into the mix, particularly as they realize that they may help shore up tight consumer protection budgets with settlement payments in privacy cases.[14] A company navigating the regulatory privacy waters has to be mindful of multiple different icebergs, and it may not be immediately obvious which iceberg poses the greatest threat to the company ship.

[13] *In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, IP-Enabled Services, FCC 07-22, at ¶¶ 54-59 (April 2, 2007), https://apps.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf.

[14] The stipulated final judgment in the Comcast case provides that $3 million of the penalty amount is allocated "for the exclusive use of the Office of the California Attorney General for the investigation, prosecution, and education of the public regarding privacy issues." *See* Final Judgment *supra* note 4, at ¶ 13.

FTC Begins "Start with Security" Conference Series

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

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

Jonathan Adams
Associate, San Francisco
jadams@wsgr.com

On September 9, 2015, the Federal Trade Commission (FTC) held its first "Start with Security" conference at the University of California Hastings College of the Law in San Francisco. The conference was the first in a series of events hosted by the agency intended to provide additional guidance to businesses regarding how to keep consumers' information secure.

The FTC's San Francisco event was aimed primarily at start-ups and software developers, with panels focusing on building a culture of security, scaling security during periods of rapid growth, investing in security, vulnerability disclosure and response, and implementing security features. The panels were each moderated by a staff attorney from the FTC's Division of Privacy and Identity Protection, with panelists hailing primarily from Silicon Valley tech companies. Each panel is summarized below.

Panel One: Starting Up Security

The first panel of the day featured Devdatta Akhawe from Dropbox, Jonathan Carter from OWASP, Frank Kim from SANS Institute, and Window Snyder from Fastly. The panel discussed how start-ups can build a culture of security and develop security expertise. Specifically, the panel examined: (1) the importance of start-up founders and executives championing security at their companies; (2) how start-ups can build internal security expertise by seeking out engineers with an interest in security and enabling them to become security evangelists; (3) how start-ups can leverage existing free and proprietary security resources such as OWASP, BSides, and SANS; (4) how to integrate threat modeling into development and to consider potential threats early in the development cycle; and (5) leveraging existing secure software frameworks and building secure abstractions for developers.

The panel also discussed cross-site scripting (XSS) attacks as a case study. XSS attacks typically involve an attacker injecting malicious code into a webpage on a target organization's website. When users visit the page, their browsers execute the malicious code, which may then steal information from the users, do other things the users did not authorize, or otherwise inject malware into the users' machines. To mitigate XSS attacks, the panel discussed verifying all data coming from a user's web browser before trusting it and HTML encoding data before sending it to a user's web browser. The panel also recommended consulting the OWASP XSS Prevention Cheat Sheet for additional mitigation methods. Finally, the panel discussed using training to help prevent XSS attacks, specifically through training developers to think like attackers and eliminate software flaws before they make it to production environments.

Continued on page 9...

FTC Begins "Start with Security" Conference Series . . . *(continued from page 8)*

Panel Two: Scaling Security

The panelists for the second panel were Michael Coates from Twitter, Zane Lackey from Signal Sciences, and Jeff Williams from Contrast Security. The panel focused on how to integrate security into modern agile software development methods and how to make security scalable. The panel discussed providing security training to all developers, doing security in small chunks throughout the development process, and having a company's security team create tools for developers to build secure code.

The panel also discussed how to leverage existing internal resources to improve security. For example, the panel discussed using existing performance and outage logs to monitor for unusual activity and potential security issues. Additionally, the panel provided examples of using existing development dashboards and code check-in tools to also scan for security issues, such as XSS vulnerabilities. Finally, the panel discussed methods of verifying that security protections are in place, including through implementing continuous alerts to provide feedback after code has been deployed.

A "Fireside Chat" Between Ashkan Soltani and Arun Mathew

Midway through the conference, FTC Chief Technologist Ashkan Soltani engaged in a "fireside chat" with Arun Mathew of Accel Partners to discuss how venture capital firms perceive security risks relating to start-ups and other emerging companies. Soltani and Mathew both emphasized that emerging companies should invest in security, as their potential investors in the venture capital and private markets increasingly perceive data security as a requisite component of any data-intensive business. Soltani and Mathew explained their view that appropriately addressing security is necessary to avoid the fallout from a data security incident, which could lead to negative press, soured customer relationships, government inquires and litigation, and investor skepticism. Mathew suggested that many venture capital firms are now evaluating emerging companies' approaches to security when reviewing their businesses for investment, with an eye toward understanding whether the companies have adequately invested in security and appropriately built security safeguards into their operations and products. Specifically, he said they consider whether start-ups have a culture of security, a budget set aside for security, and an internal process to consider security.

Panel Three: Bugs and Bounties

The third panel of the day featured Raymond Forbes from Mozilla, Paul Moreno from Pinterest, and Kaite Moussouris from HackerOne. The panel focused on vulnerability response and how companies can set up processes for receiving and responding to bug reports. Panelists pointed to existing vulnerability disclosure and handling frameworks such as ISO 29147 and ISO 30111 as processes that companies should follow. At a basic level, these involve establishing a method for securely receiving vulnerability reports, verifying and investigating reports received, communicating with bug reporters, developing security updates, and using the knowledge gained in this process to improve the software development lifecycle.

The panel also discussed whether and when it makes sense for a company to offer compensation for vulnerability reports. Specifically, the panel recommended that companies consider what scope they want to put on a bounty program (i.e., the domains, apps, versions, and types of bugs to which the program should apply), what incentives they want to offer (e.g., cash, publicity), and whether they have the time and resources to devote to a bounty program. The panel also covered the history of bounty programs, noting that although they are still relatively rare, more companies have been adopting them in recent years.

Panel Four: Beyond Bugs

The panelists for the final panel of the day were Pierre Far from Google, Jon Oberheide from Duo Security, and Yan Zhu from Yahoo. The panel discussed how to implement several technologies designed to mitigate large categories of attacks. For example, the panel discussed deploying HTTPS across an organization's entire website, rather than just sensitive areas, to protect against unsecured HTTP sniffing attacks. The panel also discussed the costs of implementing transport layer security (TLS) and projects in development that are designed to reduce those costs, such as Let's Encrypt. Additionally, the panel discussed the tradeoffs of implementing multifactor authentication, including balancing the additional protection it can provide against the additional friction it adds for users. Finally, the panel discussed different methods for implementing content security policies to mitigate the risk of XSS attacks.

Conclusion

Organizations should pay close attention to the FTC's Start with Security initiative, as guidance the FTC promulgates provides valuable insight into the agency's thinking on security issues. Moreover, FTC staff may seek to use guidance provided as a basis for what constitutes "reasonable security" in future enforcement actions. For example, the focus of several panels on XSS attacks may signal that the FTC will continue to look critically at organizations that have not taken steps to mitigate such attacks going forward. Also, given FTC staff's interest in vulnerability reporting and bounty programs, organizations should, at a minimum, ensure they have processes in place to receive vulnerability reports and may want to evaluate whether additionally creating a bounty program makes sense for the organization. Indeed, both failures to protect against XSS attacks and to implement processes for receiving and addressing third party vulnerability reports have been cited in prior FTC complaints.[1] Thus, while there is certainly no one-size-fits-all solution to data security, organizations should prioritize evaluating issues that the FTC has flagged as important in its guidance and prior enforcement actions.

[13] *E.g.,* Complaint, *United States v. RockYou, Inc.*, No. CV 12-1487 (N.D. Cal. March 26, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyoucmpt.pdf, Complaint, *In re* Fandango, LLC FTC No. 132 3089 (August 13, 2014), https://www.ftc.gov/system/files/documents/cases/140819fandangocmpt.pdf.

SEC Increases Focus on Cybersecurity—A Look at Recent Data Security Guidance and Enforcement

Tonia Klausner
Partner, New York
tklausner@wsgr.com

Whitney Costin
Associate, New York
wcostin@wsgr.com

In the wake of numerous cyberattacks aimed at companies spanning various industries, it is no surprise that yet another federal agency—this time the SEC—is stressing the importance of proper cybersecurity protocols for the entities it regulates. Broker-dealers, investment advisors, and others in the securities industry often have access to some of the most sensitive client and consumer financial information, making data security a high priority for the SEC.

In January of 2014, the SEC's Office of Compliance Inspections and Examinations (OCIE), announced that its examination priorities for 2014 would include a focus on cybersecurity preparedness in the securities industry.[1] In April 2014, OCIE announced that it would begin its cybersecurity initiative by conducting examinations of registered broker-dealers and investment advisors to assess the existence and efficacy of their cybersecurity protocols.[2] In January of 2015, OCIE announced its examination priorities for 2015, again identifying cybersecurity as a priority, and indicating that OCIE would expand its reviews to include transfer agents.[3] In February 2015, OCIE published the results of this first round of examinations, highlighting legal, regulatory, and compliance issues.[4] Among other things, the report noted that the vast majority of the 106 firms reviewed had suffered a cybersecurity incident, had adopted written information security policies, and had conducted periodic risk assessments, but the firms' policies relating to vendors and business partners varied greatly.[5]

On September 15, 2015, OCIE announced another round of examinations through a Risk Alert.[6] OCIE also provided information on the areas of focus for its second round of examinations.

According to OCIE, the examinations will focus in part on internal policies and procedures aimed at inhibiting attacks, such as governance and risk assessment, access rights and controls, data loss prevention, and the training of employees. Analyzing these internal policies and procedures will allow OCIE to determine, among other things, whether firm-specific controls are tailored to their business, how access to systems and data is managed, whether data monitors for unauthorized data transfers exist, and how employees are trained to engage in responsible and secure behavior.

The examinations will also focus on firm practices and controls related to vendor management. OCIE noted that over the last few years some of the largest data breaches may have resulted from hacking of third-party vendor platforms. Examining vendor involvement and management will allow OCIE to understand a firm's due diligence policies in selecting vendors, will show the level of oversight with respect to the vendor's practices, and will show how vendor employees are trained on maintaining a secure database.

Finally, the examinations will also focus on policies and procedures aimed at responding to a breach. OCIE will determine what, if any, firm and vendor action plans exist to respond to potential future breaches and the details of how those action plans will be implemented if or when future breaches occur.

The September 15, 2015, OCIE Risk Alert by no means limits OCIE's ability to inquire into other aspects of firm cybersecurity protocols, and firms should be ready to lay out their cybersecurity protocols and procedures for OCIE in great detail. To help prepare firms to respond to future OCIE requests for information, OCIE annexed a sample list of the types of documents they will likely seek. These documents include:

- Firm policies and procedures relating to the protection of customer records and information, including patch management practices
- Board minutes and briefing materials on cyber-related risks; cybersecurity incident response planning; actual cybersecurity incidents; and cybersecurity-related matters involving vendors
- Information regarding the firm's Chief Information Security Officer (CISO) or equivalent position, and other employees responsible for cybersecurity matters
- Information regarding the firm's organizational structure in regards to the positions and departments responsible for cybersecurity matters
- Information regarding the firm's periodic risk assessments, including penetration testing, vulnerability scans, and results and remediation efforts
- Policies and procedures regarding access rights and controls, as well as documentation reflecting implementation and compliance

---

[1] "Examination Priorities for 2014," OCIE, January 9, 2014, http://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf.
[2] "OCIE Cybersecurity Initiative," OCIE, *National Exam Program Risk Alert*, Vol. IV, Issue 2, April 15, 2014, https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.
[3] "Examination Priorities for 2015," OCIE, January 13, 2015, https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2015.pdf.
[4] "Cybersecurity Examination Sweep Summary," OCIE, *National Exam Program Risk Alert*, Vol. IV, Issue 4, February 3, 2015, https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.
[5] *Id.*
[6] "OCIE's 2015 Cybersecurity Examination Initiative," OCIE, *National Exam Program Risk Alert*, Vol. IV, Issue 8, September 15, 2015, https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

Continued on page 11...

SEC Increases Focus on Cybersecurity . . . *(continued from page 10)*

- Firm policies and procedures regarding devices used to access the firm's system externally (i.e., firm-issued and personal devices), including those addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices
- Firm policies and procedures relating to data loss prevention
- Firm policies and procedures relating to third-party vendor management, including documents pertaining to vendor due diligence, contracts, supervision, and risk assessments
- Records of cybersecurity training of employees
- Incident response policies, procedures, reports, and remediation efforts

OCIE has further shown its commitment to cybersecurity by recently taking enforcement action against an entity that it determined had inadequate measures in place to address cybersecurity. Specifically, on September 22, 2015, the SEC announced a settlement with investment advisor R.T. Jones Capital Equities Management based on charges that it had failed to adopt adequate cybersecurity controls. Following an investigation, the SEC determined that R.T. Jones Capital had entirely failed to adopt any written policies or procedures to safeguard consumer information hosted on its third-party web server, which may have led to the compromise of personally identifiable information of over 100,000 individuals.[7] The SEC's press release noted that federal securities laws require registered investment advisors to adopt written policies and procedures reasonably designed to protect customer records and information. Even though no apparent financial harm came to clients of R.T. Jones Capital as a result of a July 2013 hack, the SEC still charged the firm with violating its "safeguards rule."[8] Among other things, the firm failed to conduct periodic risk assessments, implement a firewall, encrypt personal information stored on its servers, or maintain an incident response plan. In addition to agreeing to come into compliance, R.T. Jones Capital agreed to pay a $75,000 penalty as part of the settlement.

Combined, these efforts reflect a commitment by the SEC to ensure that the entities it regulates take data security seriously and implement reasonable policies and procedures to protect against cyberattacks.

[7] *In the Matter of R.T. Jones Capital Equities Management, Inc.*, File No. 3-16827 (September 22, 2015), https://www.sec.gov/litigation/admin/2015/ia-4204.pdf.

[8] Marshall S. Sprung, co-chief of the SEC Enforcement Division's Asset Management Unit, commented that "[a]s we see an increasing barrage of cyber attacks on financial firms, it is important to enforce the safeguards rule even in cases like this when there is no apparent financial harm to clients." SEC Press Release, "SEC Charges Investment Advisor with Failing to Adopt Proper Cybersecurity Policies and Procedures Prior to Breach," September 22, 2015, http://www.sec.gov/news/pressrelease/2015-202.html.

PCI Security Standards Council Issues Guidance on Responding to a Data Breach

Jonathan Adams
Associate, San Francisco
jadams@wsgr.com

On September 29, 2015, the PCI Security Standard Council (PCI SSC) issued guidance regarding data breach responses for merchants and service providers who process payment cards. The PCI SSC is a global forum founded by card brands (American Express, Discover, JCB, MasterCard, and Visa), and it is responsible for the development and management of the data security standards (i.e., the PCI-DSS and the PA-DSS standards) required by the card brands' security programs. The new guidance includes the PCI SSC's recommendations on (i) how to prepare in advance of an incident to reduce risks and costs; and (ii) engaging and working with a Payment Card Industry Forensic Investigator (PFI) following a cardholder data breach.

The payment card industry continues to take steps intended to reduce credit card fraud and data security incidents, as evidenced by the roll-out of EMV-compliant cards and the October 1, 2015, shift in liability for card-present fraud to whichever party is the least EMV-compliant in a fraudulent transaction. By issuing this guidance, the PCI SSC illustrated how the payment card industry will continue to seek effective means for minimizing overall security shortcomings, in addition to allocating risk in the event of breaches.

Data Breach Preparation

The PCI SSC guidance lays out five basic steps that merchants and service providers should take to "prepare for the worst":

1. *Implementing an Incident Response Plan*. The PCI SSC explains that the development and implementation of management controls for responding to incidents are critical steps to reducing exposure following a data breach. PCI DSS Requirement 12.10 requires the implementation of an incident response plan by all organizations processing payment cards, and it is critical, in the PCI SSC's view, that this plan be "thorough, properly disseminated, read, and understood by the parties responsible," with appropriate testing procedures in place to ensure that the plan works.
2. *Limiting Data Exposure*. The PCI SSC recommends evaluating data systems to ensure that, in the event of a breach, systems may be appropriately isolated and investigated.

Continued on page 12...

PCI Security Standards Council Issues Guidance . . . *(continued from page 11)*

3. *Preparing to Notify Business Partners*. When a security vulnerability or breach is identified, it is often critical to alert relevant parties promptly. The PCI DSS recommends ensuring that any incident response plan contains appropriate contact information, such as the relevant contacts at service providers, payment card brands, and acquiring banks.
4. *Managing Third-Party Contracts*. The PCI SSC notes that service provider contracts should (i) address incident management (e.g., who will handle response and how will the parties coordinate) and (ii) address evidence-gathering or data access and review requirements, so that the parties roles in a post-breach environment are clearly defined. Following this guidance may ensure a more efficient and prompt response, particularly where breaches implicate or affect third party service provider systems.
5. *Identifying a PFI for Breach Response*. Finally, the PCI SSC recommends that organizations establish relationships with PFIs in advance of breaches, so that they will know who to contact when an incident occurs. The guidance notes, however, that there are independence requirements for PFIs, so merchants and service providers to merchants cannot engage a PFI that is already providing other PCI related services for the organization.

Engaging and Working with a PFI

As the guidance notes, card issuers may require that PCI-listed PFIs be responsible for conducting an independent forensic investigation and analysis of a breach. Each payment card brand has its own requirements for PFI engagement (which are linked to in the guidance), and taking time to understand the role of the PFI and the services that will be provided following a breach will help organizations plan for bringing in a PFI in the event that a breach occurs.

The PCI SSC guidance explains how PFIs investigate breaches, what reports are likely to be generated through their investigations, and how merchants and service providers may work with PFIs to ensure thorough investigations occur. PFIs will typically issue interim and final reports on incidents, which will be made available to the merchant's acquiring bank and to the payment brands, and will issue to the merchant a series of recommendations regarding containment and securing cardholder data. These recommendations are intended to supplement (and not stand in place of) the merchant's existing incident response plan, and the PCI SSC stresses the importance of following the recommendations as soon as practicable to reduce further risks to the cardholder data.

Finally, the PCI SSC guidance provides some comments on how merchants and their service providers can assist PFIs in evaluating and remediating incidents. The PCI SSC explains basic steps that organizations should take to prevent further data compromise while appropriately preserving evidence relating to the system. Beyond evidence preservation and cardholder data risk reduction, the PCI SSC also recommends that merchants and their service providers ensure that appropriate facilities and personnel are made available to PFIs to ensure effective investigations and remediation processes.

California Attorney General Includes Chief Privacy Officer Requirement in Data Privacy Settlement

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

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

California Attorney General Kamala Harris recently announced a settlement with Houzz Inc., a home design website, over allegations that the company failed to notify individuals that it was recording their phone calls with the company. While the settlement included the payment of $175,000 in penalties and fees, it also included the surprising requirement that Houzz appoint a "Chief Privacy Officer" or similar employee responsible for privacy compliance at the company. This settlement is the first time a U.S. privacy regulator has specifically included such a requirement in a privacy settlement, and it signals the importance to the California Attorney General of companies having executive management oversight for a privacy program.

Background

Houzz provides an online platform for home remodeling and design where consumers can browse design ideas, connect with home improvement professionals, and shop for curated products. The company also markets promotional services to home improvement professionals; Houzz promotes the professionals and connects them with potential customers in their area.

In its complaint, the attorney general alleged that from March 2013 to September 2013,

[1] https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-settlement-houzz-inc-over-privacy.

Continued on page 13...

California Attorney General Includes Chief Privacy . . . *(continued from page 12)*

Houzz's sales staff in its Orange County, California, office recorded all outgoing calls for quality assurance and training purposes. However, the call recipients, including professionals Houzz called to market its promotional services, were not notified that the calls were being recorded. Additionally, the attorney general alleged that from July 2013 to September 2013, the sales staff began recording all incoming calls, including calls from customers, for quality assurance and training purposes, and the company did not notify the callers that it was recording the calls. The attorney general's complaint did note that Houzz never shared any of the recordings with third parties, that a small number of Houzz's employees had access to the recordings, and only a few of the recordings were actually reviewed by employees. Nevertheless, according to the attorney general, Houzz engaged in unfair business practices because the recordings violated California's wiretapping and eavesdropping laws, which require all parties to consent the recording of phone calls.[2]

Settlement

Under the settlement, Houzz must pay $105,000 in civil penalties and $70,000 in attorneys' fees, and must comply with California's wiretapping and eavesdropping laws in the future. Surprisingly, the settlement appears to allow Houzz to keep the recordings, at least until the company determines that it is no longer appropriate to retain them. However, the company must retain the recordings in a secure location and notify the California Attorney General's office once it destroys them.
The most interesting aspect of the settlement concerns oversight of Houzz's privacy program. Within 60 days of the settlement, Houzz must designate a new or existing employee that must make good faith efforts to:

1. Be or become knowledgeable of relevant and applicable California and federal privacy statutes
2. Ensure that Houzz develops privacy policies and procedures for Houzz that are consistent with applicable state and federal privacy laws
3. Oversee Houzz's compliance with such policies and procedures

This employee may be given the title of "Privacy Officer" or "Chief Privacy Officer," but a specific title is not required. Importantly, this employee must have the authority and ability to perform the required actions and to report any significant privacy concerns to Houzz's CEO or other designated executives.

The settlement also requires Houzz to complete a privacy risk assessment that addresses Houzz's efforts to comply with applicable privacy laws governing its U.S. operations. The assessment must evaluate issues that are implicated by Houzz's business processes, its use of technology, and processes related to any third-party business partners with whom Houzz shares personal information. The risk assessment must also evaluate Houzz's efforts to mitigate or avoid any adverse effects on individuals in the United States. Once Houzz completes the assessment, it must submit a copy of the assessment's final report to the attorney general's office.

Implications

While the attorney general's inclusion of the "Chief Privacy Officer" requirement in the settlement is novel, companies handling personal information should not be surprised at the importance the attorney general places on such a role, as management and oversight is a typical requirement for comprehensive privacy and security programs.[3] Additionally, as California often plays a leading role in privacy legislation and enforcement, state attorneys general and privacy regulators may take notice of this provision and begin including similar requirements in their settlement agreements. Companies that have yet to designate and empower an employee with the responsibility for ensuring compliance with applicable federal and state privacy laws should consider doing so if they collect personal information from consumers.

---

[2] *See* Cal. Penal Code § 632(a) ("a person cannot intentionally and without the consent of all parties to a confidential communication, by means of any recording device, record the confidential communication."); Cal. Penal Code § 632.7(a)("a person cannot, without the consent of all parties to a communication, receive and intentionally record a communication between a cellular radio telephone and a landline telephone and/or between a cordless telephone and a landline telephone.").

[3] For example, the FTC's GLBA Safeguards Rule requires the designation of an employee or employees to coordinate a company's information security program. *See* 16 C.F.R. § 314.4(a). FTC privacy and data security orders often include requirements that the company designate an employee or employees to coordinate and be responsible for the privacy or security program. *See, e.g.*, Decision and Order, *In the Matter of* Facebook, Inc., FTC File No. 092-3184 (August 10, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Decision and Order, *In the Matter of* Fandango, Inc., FTC File No. 132-3089 (August 19, 2014), https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf.

No More Crying Wolf—HIPAA Audits Coming in 2016

Wendell Bartnick
Associate, Austin
wbartnick@wsgr.com

Following the conclusion of the Health Insurance Portability and Accountability Act (HIPAA) pilot audit program in 2012, speculation began about the timing of the permanent program of periodic HIPAA audits. Originally, the Department of Health and Human Service's Office of Civil Rights (OCR) scheduled the permanent audit program for 2014. However, personnel and budget limitations delayed the launch, and the year came and went without implementation of the program.

With 2015 nearing its close, advisors in the health data industry may have felt like they were crying wolf while encouraging clients to take this time to review and improve HIPAA compliance efforts given the impending audits. Finally, however, in late September 2015, the OCR announced that the permanent audit program will launch in early 2016. Reports indicate that the OCR has already sent out inquiries to covered entities confirming contact information for possible follow-up.

Why is the OCR Auditing Entities?

The HITECH Act requires that the OCR implement audits to proactively assess covered entities' compliance with the privacy and security standards set out in HIPAA. The audits provide valuable insight into areas where entities are having trouble complying with HIPAA requirements. The OCR can issue guidance addressing those problems to help all entities meet HIPAA compliance obligations. The audits also permit the OCR to assess whether the audited entities are adhering to HIPAA rules. When it finds potential non-compliance, the OCR may choose to launch an investigation and issue fines, require corrective action plans, and impose other remedies in the event HIPAA violations are found.

Which Entitites Will Be Audited?

The OCR is expected to audit approximately 400 entities, including both covered entities and business associates. The OCR will randomly select the entities, likely selecting organizations within certain segments based on size of the entity, patient volume, and other criteria.

Most Audits Likely to Be "Desk Audits"

Given the OCR's lack of resources, most of the audits are likely to be documentation reviews. However, the OCR expects to perform some on-site audits as well. The OCR may also attempt to gauge how well policies and procedures have been implemented, and it remains to be seen what evidence the OCR will want to review.

Possible Foci of Audits

OCR has communicated that it intends to focus on key common compliance failures, rather than auditing everything. The findings from the pilot audit program and the settlements following data breach investigations may provide insight into the direction of the audits. The OCR is expected to release the audit protocol prior to the start of the audits to provide more guidance to audited entities. However, entities should not wait to use the audit protocols to select which HIPAA rules to direct compliance efforts toward. We believe the OCR is likely to focus on subjects such as whether:

- Security risk assessments were completed and documented (a major problem area identified during the pilot audit program)
- Policies and procedures address the vulnerabilities identified in the risk assessment
- Written policies and procedures reflect the entity's compliance efforts with HIPAA, including the Privacy and Security rules
- Device and media controls are used
- A data incident response plan is in place
- HIPAA training is given to employees
- Appropriate business associate agreements are in place

Audits Not the Only Tool in the OCR Toolbox

The OCR commonly investigates data breaches, particularly those that affect more than 500 individuals. The OCR also responds to complaints filed by patients and others. If an investigation shows an entity's failure to meet its HIPAA-related obligations, the OCR may impose civil fines, action plans, and other obligations.

What Now?

Entities required to comply with HIPAA should consider reviewing their compliance efforts immediately to identify areas of improvement and take any necessary steps to resolve issues. The OCR has indicated that when it reviews entities during audits and investigations, it will consider how well entities have historically complied with HIPAA. Therefore, entities likely benefit from long-running compliance efforts, even if such entities are not fully compliant with HIPAA. However, organizations should avoid relying too heavily on compliance efforts made years ago, as HIPAA requires entities to update their policies and procedures to mitigate risks from the security vulnerabilities identified in an annual risk assessment and from material changes to operations and business environment. The OCR may view stale policies and procedures just as negatively, given the rapid changes in technology. HIPAA compliance is an ongoing commitment, and those organizations that have well-documented policies and procedures that meet HIPAA requirements and are regularly reviewed and improved will likely have little trouble when the OCR auditors arrive.

Landmark Decision Clarifies Territorial Scope of Application of National Data Protection Laws in the EU

Sára Hoffman
Associate, Brussels
shoffman@wsgr.com

Laura De Boel
Associate, Brussels
ldeboel@wsgr.com

Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com

On October 1, 2015, the Court of Justice of the European Union (CJEU), which is the EU's highest court, delivered its judgment in Case C-230/14—*Weltimmo*.[1] The CJEU ruling is a landmark decision in determining the territorial scope of application of national data protection laws and the competence of national Data Protection Authorities (DPAs) in the EU.

All 28 countries of the EU have their own national data protection laws. The territorial scope of application of these laws often raises questions for companies doing business in multiple EU countries. The main rule states that the national data protection law of a certain EU country applies if data processing is "carried out in the context of the activities of an establishment" of the data controller in that EU country. If the data controller is not established in the EU, but makes use of "equipment" in a certain EU country to process personal data, the national data protection law of that EU country will apply. The *Weltimmo* case provides some clarity on how to determine the application of EU data protection law when the data controller is established in the EU.

This article informs you about the facts, key findings, and implications of *Weltimmo*.

Facts

Weltimmo, a Slovakian company, operated a real estate website that allowed subscribers to list and advertise real estate for sale in Hungary. Weltimmo offered a free trial period to Hungarian advertisers, but did not deregister the advertisers that opted out at the end of the trial period. Instead, Weltimmo sent the advertisers invoices and forwarded their personal data to debt collectors.

When the Hungarian advertisers complained about these practices to the Hungarian DPA, the DPA fined Weltimmo with 10 million HUF (approximately $34,500) for breach of Hungarian data protection law. Weltimmo appealed and obtained the annulment of the DPA's decision. The case was then brought before the highest court in Hungary, which asked the CJEU to clarify whether or not Hungarian data protection law applied to the matter. Weltimmo argued that Hungarian data protection law did not apply, since Weltimmo did not have a registered office or branch in Hungary, and was therefore not *established* in Hungary.

Key Findings

The CJEU decided that Weltimmo was established in Hungary and that Hungarian data protection law applied to the matter. Below are the key findings of the case.

- *Definition of Establishment*. The court clarified the concept of "establishment." It is sufficient to have some stable arrangements to provide services in an EU country in order to be considered to have an establishment there. Having a representative in the country (in this case, local debt collectors acting on behalf of Weltimmo) may be enough. Having a postal address and a bank account in the country are additional factors to consider. The court also took into consideration the fact that Weltimmo's service, in the context of what personal data was processed, was targeted to Hungary (i.e., the website featured properties in Hungary and was written in Hungarian). Finally, the court specified that the nationality of the individuals concerned by the data processing is irrelevant for the determination of the applicable national data protection law.
- *National DPA Jurisdiction Hinges on Establishment*. The court stated that a national DPA is competent for the companies that are established in its jurisdiction. It cannot impose penalties on companies established outside its own country. Therefore, if a company does not have an establishment the EU country where the infringing act occurred, the DPA of that country may not impose penalties. Instead, it should request the DPA of the EU country where the company is established to investigate the matter and to potentially sanction the company in accordance with its own applicable data protection law.

Implications

Since the court's threshold for having an "establishment" is relatively low, businesses that carry out data processing activities in multiple EU countries should beware that they can be considered to be established in several EU countries, even if they don't have legal entities there. It may be sufficient to target individuals in a certain EU country and to work with people on the ground (e.g., debt collectors) to be considered to have an establishment in that EU country. In the EU, the same data processing activity may thus be subject to different national data protection laws that are enforced by different DPAs, if the activity involves multiple EU markets. In light of this judgement, companies should reassess their strategy for compliance with multiple local data protection laws.

[1] The judgment is available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=168944&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=711640.

Upcoming Industry Events Featuring WSGR Privacy & Data Protection Professionals

IAPP Europe Data Protection Congress
December 2-3, 2015
Brussels

- On December 2, WSGR Of Counsel Cédric Burton will speak as part of the Privacy in Conversation series on "A World Without Safe Harbor: What Now?" Other panelists include Florence Raynal, head of the Department of European and International Affairs at the CNIL, and Ted Dean, Deputy Assistant Secretary for Services, International Trade Administration, from the U.S. Department of Commerce. Cédric will also speak December 3 on a panel discussing data anonymization, pseudonymization, and other de-identification techniques.

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