Skadden

PRIVACY & CYBERSECURITY UPDATE

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP & AFFILIATES

December 2013

European Commission Proposes Changes to the US-EU Safe Harbor

In our November *Privacy & Cybersecurity Update*,[1] we reported that the European Commission was undertaking a review of the U.S.-EU Safe Harbor, one of the frameworks available to U.S. companies to satisfy the "adequacy" requirement for transborder data flows from the EU under the EU Data Directive. This concern was triggered, in no small part, by revelations of U.S. surveillance programs. On November 27, 2013, the European Commission issued its report, setting forth 13 recommendations to improve the protection afforded to EU residents under the Safe Harbor. The report came as a relief to some who were concerned that the European Commission might propose a wholesale revision to the Safe Harbor process or even advocate for its elimination.

The Commission noted that a review of the Safe Harbor process was warranted at this time because of the exponential growth in data flows, the importance of those data flows in a global economy; the increase in the number of companies relying on the Safe Harbor and the revelation of US surveillance programs. Indeed, the Commission noted that all companies involved in the US PRISM surveillance program were Safe Harbor certified. In addition, the Commission acknowledged that some data protection authorities found the Safe Harbor to be too general, and overly reliant on self-certification and self-regulation, while some industries felt that a lack of enforcement of Safe Harbor violations provided a competitive advantage to U.S. entities.

The Commission's proposals focus on four key areas: transparency; redress; enforcement; and, not surprisingly given the current environment, access by U.S. authorities.

Transparency Recommendations

- **Public disclosure of privacy policies**. Although the Safe Harbor requires that companies make their privacy policies publicly available, many have not. In addition, many policies are not presented in a "consumer friendly and easily readable format." The Commission therefore recommends that privacy policies be made available on a company's website in clear and conspicuous language. The Commission notes that the Department of Commerce has made such disclosures mandatory since March 2013, but urges the Department of Commerce to be more stringent in its enforcement
- **Privacy policies should link to the safe harbor website**. The Commission makes this recommendation because it believes it will help eliminate false claims of certification and also allow individuals to quickly check if a company is actually listed as being certified.
- **Disclosure of subcontractor relationships**. The Commission notes the increase in the use of subcontractors, especially with respect to cloud computing. While such onward transfers are permissible, the Commission believes that in the interest of transparency, certified companies should disclose their subcontracting relationships to the Department of Commerce and make public any privacy safeguards that have been imposed.
- **Disclosure of noncompliant companies**. The Commission is particularly concerned with entities that claim to be certified when, in fact, they no longer are. The

1 *See* http://www.skadden.com/newsletters/Privacy_&_Cybersecurity_Update_November_2013.pdf.

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or your regular Skadden contact.

Stuart D. Levi, New York
212.735.2750
stuart.levi@skadden.com

James S. Talbot
212.735.4133
james.talbot@skadden.com

* * *

Four Times Square
New York, NY 10036
Telephone: 212.735.3000

WWW.SKADDEN.COM

Commission therefore recommends that the Department of Commerce publish a "not current" list of Safe Harbor members who are not fulfilling their obligations. The Commission notes that in November 2013, the Department of Commerce began a process of notifying Safe Harbor participants one month before their recertification date of what they need to do to recertify. The notice also reminds companies that they will be subject to FTC enforcement activity if they choose not to recertify, but continue to claim to be certified

Redress Recommendations

- **The role of ADR**. The Safe Harbor requires that a Safe Harbor participant make available a "readily available and affordable" recourse mechanism. Many participants rely on alternative dispute resolution Providers. The Commission has found, however, that ADR is often expensive and difficult to monitor. It, therefore, made three recommendations in this area. First, Safe Harbor participants should link to the ADR provider (or the EU panel if that method is chosen) so that a data subject can easily reach out to them. Second, the Commission suggests that certain ADR panels (which can charge $250 for filing a complaint) may be too expensive to meet the "readily available and affordable" standard. Third, the Commission proposes that the Department of Commerce monitor ADR providers more systematically concerning the accessibility of information they provide.

Enforcement Recommendations

One of the biggest complaints that data human rights advocates have had about the Safe Harbor in EU companies is a lack of any meaningful enforcement. While the Commission acknowledges that the Federal Trade Commission has brought some enforcement actions, there still have been few in number. The Commission therefore made four recommendations in the area of enforcement:

- The Department of Commerce should conduct random investigations of a sampling of Safe Harbor participants to assess compliance with their privacy policies (even extending beyond compliance with Safe Harbor).
- If a Safe Harbor participant is found to be non-complaint, there should be a follow-up investigation after one year.
- The Department of Commerce should inform the applicable data protection authority if it has doubts about a company's compliance.
- False claims of adhering to the Safe Harbor should continue to be investigated.

Recommendations Concerning Access by US Authorities

As noted above, one of the key triggers of the Commission's Safe Harbor review was the revelation that the U.S. government was conducting surveillance of certain U.S. and EU residents. The Commission also notes that EU data subjects have no recourse against government intrusions, and that these data subjects (and their U.S. counterparts) do not have the ability to seek redress for such intrusions. It is, therefore, no surprise that two of the recommendations deal with this issue.

- **Privacy policies of Safe Harbor participants should disclose the extent to which U.S. law allows the government to collect and process data transferred under the Safe Harbor**. Of all the Commission's recommendations, this seems to be the least likely to gain any traction. Companies will be loath to include specific statements about how their data might be accessed by the government, while broad general statements about the possibility of such access would accomplish little. Still, this recommendation reflects the Commission's concern in this area.
- **The National Security Exception to the Safe Harbor should be used only as strictly necessary**.

Despite the report's attempts to strengthen enforcement of the Safe Harbor, many critics of the framework are still not satisfied. Monique Goyens, the director general of The European Consumer

Organization, commented that, "better enforcement is crucial and we're glad to see that being examined. But the ability of companies to self-certify as offering 'Safe Harbor' is unjustifiable and remains inexplicably outside the review. It is hard to see the purpose of proceeding without tackling such basic flaws and perhaps the time has come to put the Safe Harbor agreement to one side and move on."

Practice Points

Even if none of the Commission's recommendations are adopted, companies should expect renewed focus on Safe Harbor compliance by the Department of Commerce and the EU, if for no other reason than to assure the European Commission and European data protection authorities that the Safe Harbor offers a viable means of protecting EU data. Companies that certify to the Safe Harbor should there remain even more vigilant about their compliance, and should be sure to recertify each year. Companies also should review the Department of Commerce's new requirements for Safe Harbor compliance, which include making their privacy policies accessible on their website and including links to the Department of Commerce Safe Harbor list. In addition, companies that rely on Safe Harbor certification should remain abreast of developments in the EU regarding the Safe Harbor.

LabMD Challenges FTC Authority to Enforce Data Security Policies

LabMD, an Atlanta-based cancer detection company, is challenging the FTC's jurisdiction over a company's data security practices. Like Wyndham Hotels, which has been engaged in a similar legal battle with the FTC since June 2012, LabMD has asserted that since there is no definitive legal standard for security, there is, in effect, nothing for the FTC to enforce. The challenges by LabMD and Wyndham are significant because they come at a time when the FTC is seeking to expand its role in the cybersecurity arena.

LabMD suffered two separate data breaches, affecting information belonging to approximately 10,000 consumers. The first breach was uncovered in 2008 when a file with billing information for more than 9,000 customers was found on Limewire, a P2P sharing site that had been installed on a billing computer. The second breach was uncovered in 2012 when law enforcement officers in Sacramento, Calif., found documents containing information for approximately 500 LabMD customers in the possession of identity thieves.[2] In August 2013, the FTC filed an action against LabMD under Section 5 of the FTC Act alleging that LabMD failed to implement appropriate data protection measures, which caused injury to consumers.

LabMD, like Wyndham, moved to dismiss the complaint, arguing that Section 5 does not give the FTC authority to determine whether data-security protections are "unfair" in the absence of definitive federal legislation in the area.[3] LabMD also asserted that even if the FTC has general authority to regulate data privacy under Section 5, it does not have authority in the heath-information area because Congress delegated sole enforcement authority in that area to the Department of Health and Human Services under HIPAA and HITECH.[4]

---

2 FTC Complaint, In the Matter of LabMD, Inc., Docket No. 9357 (Aug. 29, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.

3 Wyndham Motion to Dismiss, *FTC v. Wyndham Worldwide*, Civil Action No. 2:13-cv-01887-ES-SCM (D.NJ, June 17, 2013)

4 LabMD Motion to Dismiss, In the Matter of LabMD, Inc., Docket No. 9357 (Nov. 12, 2013), available at http://www.ftc.gov/sites/default/files/documents/cases/131112respondlabmdmodiscomplaintdatyadminproceed.pdf. HIPAA is the Health Insurance Portability and Accountability Act, and HITECH is the Health Information Technology for Economic and Clinical Health Act.

The complaint has not yet been made public because LabMD has asserted it contains confidential business information. In a public version of the complaint that has been redacted due to LabMD's assertions that it contains confidential information, the FTC stated that LabMD:

- did not implement or maintain a comprehensive data security program to protect this information;
- did not use readily available measures to identify commonly known or reasonably foreseeable security risks and vulnerabilities to this information;
- did not use adequate measures to prevent employees from accessing personal information not needed to perform their jobs;
- did not adequately train employees on basic security practices; and
- did not use readily available measures to prevent and detect unauthorized access to personal information.[5]

Practice Point

Without knowing LabMD's specific practices, it is difficult to assess at this juncture whether the company's security procedures were egregiously below generally accepted industry standards. However, the FTC allegations provide an important roadmap of those areas to which companies should pay particular attention. Specially, companies should make sure that they have a comprehensive security policy and that employees are trained on that policy. Employees also should only have access to personal information on a need to know basis. Finally, while LabMD is correct that there is no federal security standard, companies should be mindful of industry standards.

FTC Sets Privacy and Data Security Agenda for 2014

As we have reported in this and previous newsletters, much of the enforcement activity with respect to privacy and data security has occurred through the FTC. It is therefore important to review the FTC's announced roadmap for what it sees as the key privacy and security issues in 2014.

On December 6, 2013, Jessica Rich, director of the Bureau of Consumer Protection at the FTC, outlined some of the FTC's key areas of concerns. Rich cautioned that despite the benefits that data crunching can bring, consumers are increasingly wary of how data is being used and the security offered by vendors. She also noted that failing to provide adequate levels of security can harm a business' reputation and valuation. And, on the other side, robust privacy and security measures are being embraced by consumers and can be part of a broader business strategy.

With respect to a 2014 agenda, Rich indicated that the FTC had "no intention of slowing down" and that the FTC's privacy work would "continue at a rapid pace in the coming year." The FTC agenda will focus on three broad areas: big data; mobile devices; and protection of sensitive data. Within these areas, the FTC will keep reminding companies about the three goals articulated in the FTC's 2012 privacy report: privacy-by-design, transparency and simplified choice.

Big Data

The FTC's concern about Big Data is that it constitutes the pooling of vast stores of data, often without consumer knowledge, let alone consent. In addition, large databases create greater security risks in the event of breach and allow companies to make inferences about consumers that may not be true. In 2014, the FTC is slated to release a report on "data brokers" — organizations that collect and sell consumer information, typically without any interaction with the

5 FTC Files Complaint Against LabMD for Failing to Protect Consumers' Privacy, FTC Press release dated Aug. 29, 2013, available at http://www.ftc.gov/news-events/press-releases/2013/08/ftc-files-complaint-against-labmd-failing-protect-consumers.

consumer. Since consumers are in the dark about these brokers, they do not know how to access their data or challenge their collection. The FTC plans in its report to shed light on this industry and its practices. The FTC will also be releasing a report on the practice of ISPs and other entities to engage in "comprehensive data collection," *i.e.*, collecting data about a user continuously and over multiple sites.

In connection with this education process, the FTC announced a spring seminar series that will focus on three areas:

- **Mobile device tracking in retail stores and other businesses**. This seminar is open to the public and will take place on February 19, 2014, from 10 a.m. to 12 p.m. at the FTC's Conference Center, 601 New Jersey Ave., NW, Washington, DC. The FTC has invited public comments to be submitted by March 19, 2014.
- **The use of predictive scoring to predict consumer behavior**. This seminar is open to the public and will take place on March 19, 2014, at the FTC's Conference Center. The seminar will focus, among other areas, on whether consumers should have access to the underlying data on which they are scored, and whether the Fair Credit Reporting Act should govern the use of such scoring. The FTC has invited public comments to be submitted by April 19, 2014.
- **The health app industry**. The FTC has noted that consumers are increasingly providing their health data for apps that offer a variety of monitoring and tracking services. The FTC has not yet set a date for this seminar.

Finally, Rich announced that the FTC will continue to enforce the Fair Credit Reporting Act vigorously since it often provides the tools to protect consumers against the misuse of Big Data.

Mobile Technology and Connected Devices

In 2014, the FTC will be releasing its report on mobile security, based on a workshop it held in June 2013. The report is expected to highlight the privacy issues raised by security risks with mobile devices. Rich also highlighted the FTC's enforcement action against HTC America as an example of the FTC's increasing role in mobile security.[6]

Rich's discussion of mobile also covered the so-called "Internet of Things" — the ability of users to connect remotely with numerous products — such as cars, themostats, televisions, etc. The FTC's concern in this area is that it is difficult to offer consumers notice and choice options given the manner in which these systems are configured. In addition, manufacturers in this area are less familiar with data privacy and security and, therefore, less likely to incorporate "privacy by design" into their manufacturing processes. In 2013, the FTC settled an action against TRENDnet, a manufacturer of home security cameras, for failing to provide adequate security for its cameras.[7] The FTC will be issuing a report on the Internet of Things in 2014 and is accepting public comments through January 10.

Sensitive Data

The FTC identifies three categories of sensitive data: data involving children, health data and financial data. In July 2013, the final Children's Online Privacy Protection Act (COPPA) went into effect.[8] Rich noted that in 2013, the FTC did not actively pursue violators of the new rule as companies sought to adopt to its new requirements. However, Rich cautioned that the FTC will "ramp up enforcement" of COPPA in 2014.

---

6 *See* http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_%20April%202013.pdf.

7 *See* http://www.skadden.com/newsletters/Privacy_Cybersecurity_Alert_October_2013.pdf.

8 *See* http://www.skadden.com/insights/privacy-update-ftc-strengthens-online-child-privacy-regulations.

In the healthcare area, the FTC brought two actions in 2013. One was against Cbr, a cord blood bank, for failing to protect unencrypted personal information that was stored in a laptop and was stolen out of a car. More recently, the FTC brought an action against LabMD, discussed above in this newsletter.

Finally, Rich reviewed the action brought by the FTC against Wyndham Hotels for failing to protect consumer credit card information against a security breach.

Perhaps most importantly, Rich addressed, albeit briefly, the concern among many observers that the FTC is enforcing a security standard that does not formally exist. The concern is that that any security breach is arguably a failure to provide adequate security, and therefore could expose a company to an FTC complaint. Rich stated that the standard in security cases is not "perfection," but rather "reasonable security." Nonetheless, many will continue to be concerned that there is no way to decipher what constitutes "reasonable" security in a world where security standards are constantly evolving and where hackers grow increasingly sophisticated.

Future Legislation

Rich ended her remarks by surveying the potential for privacy and security legislation. Interestingly, Rich conceded that while an omnibus privacy law would benefit companies and consumers alike, "privacy legislation seems like a far-off goal right now" given the numerous conflicting opinions on the optimal approach. However, Rich noted that there is less disagreement about the need for data security legislation, and urged that such legislation be enacted in 2014.