Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

THE WSGR DATA ADVISOR

JULY 2015

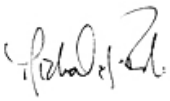
Welcome

Data collection, storage, and use permeate everything our clients do. Whether it's collecting data about your customers to provide a more personalized shopping experience, modeling third-party data to deliver more cost-effective advertising, leveraging health and sensor data to help your customers live healthier lives, or developing new innovations in the Internet of Things, data drives the modern economy. With this in mind, we've transformed our *Eye on Privacy* to *The WSGR Data Advisor* to reflect our focus on advising on everything data. Every day, Wilson Sonsini Goodrich & Rosati's privacy and data protection practice helps companies navigate the complex and ever-changing set of laws, regulations, and industry standards that govern the collection, storage, and use of data. We intend for *The WSGR Data Advisor* to be a source of unique insights on data from our experienced and accomplished team. Watch this space for more changes to come and news on upcoming events we're hosting or attending.

We'd also like to invite you to join us on July 15 for a special webinar presentation on the latest developments with the proposed EU Data Protection Regulation. More information can be found in the upcoming events section on page 16.

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

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



Michael Rubin
Partner, San Francisco
mrubin@wsgr.com

Navigating Public Company Cybersecurity Obligations: Advising Boards and Disclosing to Investors

Matthew Staples
Associate, Seattle
mstaples@wsgr.com

Jonathan Adams
Associate, San Francisco
jadams@wsgr.com

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

In light of numerous costly security breaches affecting disparate sectors of the American economy, public companies—ranging from merchants like Target Corporation and The Home Depot to technology firms like Adobe Systems, and from entertainment companies like Sony Entertainment to insurers like Anthem Blue Cross, to name a few examples—are under increased pressure to ensure that cyber risks are appropriately evaluated, addressed, and disclosed to investors. Because of the increasing number and cost of data security incidents, the U.S. Securities and Exchange Commission (SEC) has taken an active role in advising public companies on how to appropriately manage and disclose cyber risks. SEC cyber risk guidance to date, outside of advice specific to the financial services industry, relates to: (i) the responsibilities and duties that boards of public companies must bear with regard to cyber risk; and (ii) the manner in which public companies should disclose (when appropriate) the relevant cyber risks in company filings with the SEC.

The Role of the Board of Directors

In his 2014 remarks, "Board of Directors, Corporate Governance, and Cyber-Risks: Sharpening the Focus," SEC Commissioner Luis A. Aguilar provided a useful framework for boards of directors and the attorneys advising public companies to follow when contemplating cybersecurity matters. As Commissioner Aguilar noted, a board owes broad duties to the corporation, and has a significant role in corporate governance and overseeing risk management, including cyber risks. To Aguilar—and likely the SEC—the board's role in addressing cyber risk is akin

In This Issue

Navigating Public Company Cybersecurity . . . *(continued from page 1)*

to its role in addressing and managing other material risks to a corporation, whether they are financial, regulatory, or business-related. Thus, although a public company's management has the primary day-to-day responsibility for managing risks, public company boards of directors must ensure that the company has established appropriate risk management programs and that the company's management is implementing those programs appropriately.

Despite the obvious need for board involvement in cybersecurity matters, as Commissioner Aguilar noted in his remarks, many boards may be failing to exercise sufficient oversight or failing to devote appropriate energy or resources to address[1] cybersecurity.[1] Surveys continue to suggest that, despite the enterprise-level cyber risks facing many public companies, many boards are not undertaking cyber risk oversight actions (including basic measures, such as reviewing annual budgets for privacy and IT security programs, assigning managerial responsibilities relating to security, or receiving reports of IT risks).[2] Taking corrective action on this "low-hanging fruit" could go a long way in reducing the quotidian cybersecurity risks facing public companies.

Beyond staying minimally informed and setting appropriate budgets, boards can take (and many have taken) more focused measures to address cybersecurity risks. Boards that may lack the requisite expertise to determine whether a company's management is appropriately addressing cybersecurity matters (as opposed to, for instance, financial controls required under Sarbanes-Oxley, with which a board may have greater familiarity and knowledge) may benefit from receiving cybersecurity- and privacy-related education. When a company, based on its business or risk profile, is more likely than not to face cybersecurity risks, it may be sensible for the company to ensure that some directors maintain a suitable understanding of the relevant technological issues and risks. Beyond internal education, boards can also take steps to ensure that appropriate cybersecurity audits are conducted on a regular basis. Many boards have gone further and appointed board-level committees that are responsible for privacy and cybersecurity risks—the number of corporations with such specialized risk committees increased from 8 percent to 48 percent between 2008 and 2014.[3] Ultimately, as part of the board's general oversight function, directors should assess the adequacy of their company's cybersecurity measures, taking into account the company's cybersecurity risk profile, who within the company's management has primary responsibility for risk oversight, how the company plans to manage cybersecurity risks, and the company's insurance coverage for losses and costs resulting from cyberattacks.

Boards must also take appropriate measures to ensure cyber incident preparedness in their companies. Unlike many other crises a public company may face, cyberattacks require near-immediate action: time is of the essence in detecting, analyzing, containing, and responding to system infiltrations or other attacks. Thus, boards should ensure that their companies' management has developed well-designed, thought-out, and implementable response plans to address cyberattacks. Boards should also ensure that appropriate staff is in place to monitor IT systems and respond to security issues. Evidence suggests that companies that employ full-time chief information security officers (or equivalent positions) who report directly to management were able to detect more security incidents and report lower average financial losses per incident.[4] By ensuring that companies have hired the right people, and that those employees have appropriate budgets and plans for managing and responding to risks, boards can play an appropriate role in significantly reducing enterprise risk.[5]

Boards that fail to pay appropriate attention to cybersecurity matters may face scrutiny, not only from regulators but also from their companies' investors. Failure by a public company to appropriately address cyberattacks can lead not only to management changes—as seen with Target Corporation and Sony—but also to investor efforts to unseat board members. For example, in the wake of the Target Corporation cyberattack, a prominent proxy advisory firm encouraged the ouster of most of the Target directors in light of their perceived "failure . . . to ensure appropriate management of [the] risks" relating to the cyberattack.[6] Likewise, shareholder derivative suits against companies and their officers and directors may be launched in the wake of a cybersecurity incident. For instance, the directors and officers of Target Corporation and Wyndham Hotels have faced derivative litigation in the past year as a result of those companies' cybersecurity failures.[7]

Cyber Risks in Public Filings

In October 2011, the SEC Division of Corporation Finance released CF Disclosure Guidance: Topic No. 2 (CF Guidance) that outlined the division's view of how public companies should discuss cybersecurity matters in their public filings.[8] As the division notes, the CF Guidance is "consistent with the relevant disclosure considerations that arise in connection with any business risk," and that federal securities laws do not require companies to make "detailed disclosures [that] could compromise cybersecurity efforts—for

---

[1] Although boards are playing an increased role in overseeing cybersecurity matters in their companies, a 2014 survey found that a majority of boards have never discussed engaging an outside security expert, cyber risk disclosures in response to SEC guidance, an actual breach of the company's security, the company's cyber insurance coverage, the development of the Department of Homeland Security/National Institute for Standards in Technology (NIST) cybersecurity framework, or the need to designate a chief information security officer. PricewaterhouseCoopers LLP, *2014 Annual Corporate Directors Survey: Trends Shaping Governance and the Board of the Future* (PwC Survey), at 32, http://www.pwc.com/us/en/corporate-governance/annual-corporate-directors-survey/assets/annual-corporate-directors-survey-full-report-pwc.pdf. Fortunately, the focus on cybersecurity is increasing among directors: the same study found that 65 percent of directors want to increase their boards' focus on cybersecurity matters. *Id.* at 6.

[2] *See, e.g.*, Steven P. Blonder, "How closely is the board paying attention to cyber risks?" *Inside Counsel*, April 9, 2014, *available at* http://www.insidecounsel.com/2014/04/09/how-closely-is-the-board-paying-attention-to-cyber.

[3] Deloitte Audit Committee Brief, Cybersecurity and the audit committee (Aug. 2013), at 2, *available at* http://deloitte.wsj.com/cfo/files/2013/08/ACBrief_August2013.pdf.

[4] PricewaterhouseCoopers LLP, *The Global State of Information Security Survey 2014*, at 4, *available at* http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml. The PwC Survey also noted that all of the following contributed to improved cybersecurity response results: (i) having an overall cybersecurity strategy; (ii) reviewing the effectiveness of security measures within the past year; and (iii) having an understanding of recent cybersecurity events.

[5] This is an area where many boards continue to struggle: According to the 2014 PwC survey, "nearly half of directors have not discussed their company's crisis response plan in the event of a security breach, and more than two-thirds have not discussed their company's cybersecurity insurance coverage." PwC Survey at 8.

Continued on page 3...

Navigating Public Company Cybersecurity . . . *(continued from page 2)*

example, by providing a 'roadmap' for those who seek to infiltrate a registrant's network security." Appropriate disclosures are required, however, because of the substantial costs and other negative consequences that a public company may suffer, which may include:

- Remediation costs, including potential liability for stolen assets or information and repairing system damage that may have been caused or incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
- Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
- Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
- Litigation; and
- Reputational damage adversely affecting customer or investor confidence.

In large part, these disclosures are required because federal securities laws are "designed to elicit disclosure of timely, comprehensive, and accurate information about risks and events that a reasonable investor would consider important to an investment decision."[9] Although no securities laws or SEC rules refer explicitly to cybersecurity risks, a number of general disclosure requirements may impose an obligation on registrants to disclose such risks and incidents, and material information regarding cybersecurity risks and cyber incidents must be disclosed when necessary in order to make other required disclosures not misleading.

As a result, every public company should review its public filings on a regular basis to ensure that it is making appropriate disclosures, taking into account various factors relating to the company's business. Likewise, a company filing for its initial public offering should take the opportunity to reflect on and appropriately disclose cybersecurity matters. Cybersecurity disclosures may be needed for a variety of reasons in several sections of a company's periodic reporting disclosure or registration statement, including, among others, the following:

Although no securities laws or SEC rules refer explicitly to cybersecurity risks, a number of general disclosure requirements may impose an obligation to disclose such risks and incidents

Risk Factors. A public company should discuss cybersecurity risks in its risk factors if cybersecurity issues are among the significant factors that make an investment in the company speculative or risky. As with other risk factor disclosures governed under Regulation S-K Item 503(c), cybersecurity risk factors must adequately describe the nature of the material risks and specify how each risk affects the company, and should not include generic risks that could apply to any issuer or any offering. Ideally, cybersecurity risk factor disclosure should include an evaluation of the company's cybersecurity risks, prior cyberattacks, and likelihood of future attacks, as well as the potential costs associated with cybersecurity risks. In addition, such risk factor disclosure could include: (i) specific discussion of aspects of the company's business or operations that give rise to material cybersecurity risks and the potential costs and consequences; (ii) a description of outsourced functions presenting cybersecurity risks (and how the company addresses those risks); (iii) risks related to cybersecurity incidents that may remain undetected for an extended period (if known to the company); and (iv) a description of the company's relevant insurance coverage or lack thereof. If cybersecurity incidents have affected a company previously, those incidents should inform and be integrated into the company's disclosures to provide additional context to the disclosure.

MD&A. The SEC corporate finance division has explained that public companies should address cybersecurity risks and cyber incidents in their Management Discussion and Analysis of Financial Condition and Results of Operations (MD&A) if the costs or consequences associated with actual cyberattacks, or the risk of potential cyberattacks, represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the company's results of operations, liquidity, or financial condition, or would cause reported financial information not to be necessarily indicative of future operating results or financial condition. This could occur if a cyberattack has resulted, or could result, in the loss or exposure of material intellectual property, in which case the effects of this loss or exposure should be described. Similarly, if a cyberattack has resulted in, or could result in, increased costs or reduced revenues, the historical impact and potential outcomes should be discussed. Under the division's guidance, even material increases in cybersecurity protection costs should be discussed in the MD&A.

Description of Business. If one or more cybersecurity incidents materially affect a company's products, services, relationships with customers or suppliers, or competitive conditions, the company should disclose the effect of the incidents when describing the affected business component.

---

[6] Paul Ziobro, "Target Shareholders Should Oust Directors, ISS Says," *The Wall St. Journal*, May 28, 2014, *available at* http://online.wsj.com/article/BT-CO-20140528-709863.html.

[7] *See, e.g., Collier v. Steinhafel*, No. 0:14-cv-00266 (D. Minn. Jan. 2014), (alleging failings by Target's board and top executives); *Palkon v. Holmes*, No. 2:14-cv-01234 (D.N.J. May 2014) (alleging that, by failing to take adequate steps to safeguard customers' personal and financial information, Wyndham's board and top executives caused financial damage to the company).

[8] Although the CF Guidance is not a rule, regulation, or statement of the SEC, and the SEC has not approved of its content, the CF Guidance is a strong indication of how the SEC will proceed internally and what it will expect in a public company's reporting.

[9] CF Guidance at n.2.

Continued on page 4...

Navigating Public Company Cybersecurity . . . *(continued from page 3)*

Legal Proceedings. To the extent a material pending legal proceeding to which a company is a party involves a cybersecurity incident, the company may need to disclose information regarding this litigation in its disclosure of legal proceedings.

If cybersecurity incidents have affected a company previously, those incidents should be integrated into disclosures to provide additional context

Financial Statements. Cybersecurity risks and cybersecurity incidents may have a broad impact on a company's financial statements, depending on the nature and severity of the potential or actual incident. In attempting to mitigate cybersecurity risks, companies may incur substantial costs for software, audits, training, and other risk mitigation tools. Likewise, if a cybersecurity incident occurs, companies may seek to mitigate damages by providing customers with incentives to maintain business relationships, and may incur losses from asserted and unasserted claims, including those related to warranties, breach of contract, product recall and replacement, payment card network fines, and indemnification of counterparty losses from their remediation efforts. Cybersecurity incidents may also cause diminished future cash flows, thereby requiring consideration of impairment of certain assets including goodwill, customer-related intangible assets, trademarks, patents, capitalized software or other long-lived assets associated with hardware or software, and inventory. Public companies may not be able to immediately evaluate the impact of a cybersecurity incident and thus may be required to develop estimates to account for the various financial implications. In these cases, companies should subsequently reassess the assumptions that underlie the estimates made in preparing the financial statements, and must explain any risk or uncertainty of a reasonably possible change in its estimates in the near-term that would be material to the financial statements. Finally, if a cybersecurity incident is discovered after the balance sheet date but before the issuance of financial statements, companies should consider whether disclosure of a recognized or non-recognized subsequent event is necessary.

Disclosure Controls and Procedures. Public companies are required to provide conclusions on the effectiveness of their disclosure controls and procedures. To the extent cybersecurity incidents pose a risk to interfere with a company's ability to record, process, summarize, and report information that is required to be disclosed in filings, the company's management should consider whether this may result in any deficiencies in its disclosure controls and procedures that would render them ineffective.

The CF Guidance has ensured that companies continue to expand their disclosures relating to cybersecurity. Following a 2007 data breach that resulted in the theft of approximately 94 million credit and transactional records, TJX Companies, Inc., reported the incident in its Form 10-K filing, but with limited references (in the Introduction, as a Risk Factor, and as a Legal Proceeding). In contrast, later corporate victims of cybersecurity incidents have provided far more expansive disclosures—in some cases, companies suffering cybersecurity incidents have mentioned such incidents more than 200 times in their Forms 10-K.[10] Arguably, certain public filings may *over*-disclose in an effort to diffuse SEC scrutiny; as the CF Guidance makes clear, however, irrelevant or boilerplate disclosures do not satisfy a company's obligation to provide appropriate disclosures to investors. Every public company—and each company seeking to make public offerings—should take time to evaluate its cybersecurity risks, exposures, and potential costs to ensure that its public filings meet SEC expectations.

---

[10] *See* Heartland Payment Systems 2010 Form 10-K Report, *available at* http://www.snl.com/IRWebLinkX/file.aspx?IID=4094417&FID=10884340&O=3&OSID=9 (making nearly 250 references to the 2009 hack of its database that compromised approximately 130 million records).

FTC Updates School-Related COPPA Guidance

Maggie Lassack
Of Counsel, Washington, D.C.
mlassack@wsgr.com

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

The use of technology in classrooms across the country has exploded in recent years. This has prompted increased activity by federal and state lawmakers to enact laws to protect student privacy,[1] as well as raised numerous questions about how the Children's Online Privacy Protection Act (COPPA) applies to schools, the technologies they use, and the information they collect. The Federal Trade Commission (FTC) staff has responded to these questions by recently updating its guidance on how COPPA applies to educational institutions that collect information from children.[2] While the FTC staff did not make significant changes to its guidance, the revisions demonstrate the FTC's continued interest in protecting student privacy, highlight the various federal and state laws concerning student privacy, and serve as a reminder to educational institutions and their service providers of the importance of adequately protecting the privacy of student information.

"COPPA and Schools" FAQs Update

COPPA prohibits companies from collecting personal information from children under the age of 13 without first providing notice to parents and obtaining their verifiable consent.[3] Compliance with COPPA can be complicated for many organizations, and the FTC staff publishes a set of frequently asked questions (FAQs) to provide guidance for organizations working to comply with the law.[4] The FTC staff recently updated its "COPPA and Schools" FAQs, which are directed to educational institutions and companies that provide online services to educational institutions. The FTC staff updated FAQs M.1, M.4, and M.5 to: (i) clarify when educational institutions can consent to a website or app's collection, use or disclosure of students' personal information; (ii) identify best practices for informing parents about the collection and disclosure of students' personal information, and (iii) provide information about other federal and state laws that may protect student data. The FTC staff also removed FAQ M.6 as part of its ongoing efforts to streamline the FAQs.

FAQ M.1 explains that a school may act as the parent's agent and provide consent for a third-party website or app operator's collection and use of student information, but only when the operator collects the student information for the use and benefit of the school, and for no other commercial purpose.

The FTC staff updated FAQ M.1 to clarify that the operator "can presume that the school's authorization is based on the school having obtained the parent's consent," if the operator limits the use of the collected information to the educational context authorized by the school. The updated FAQ M.1 also recommends that, as a best practice, schools should consider providing the operator's required notices under COPPA to parents, and consider the feasibility of allowing parents to review the collected student information. The FTC staff also added language to FAQ M.1 recommending that schools ensure operators delete information they collect from students once the information is no longer needed for educational purposes.

In addition, the revised FAQ M.1 reminds organizations that state laws may also protect student data, such as laws requiring contracts between schools and service providers to include express provisions for safeguarding the privacy and security of student information or prohibiting secondary uses of student information without parental consent.[5] The revised FAQ M.1 also specifically references California's Student Online Personal Information Protection Act (SOPIPA),[6] which applies to operators of websites, online services, or mobile apps that are designed, marketed, and primarily used for K-12 school purposes. The law restricts the use of K-12 students' information for targeted advertising, profiling, or onward disclosures. It also requires operators to maintain reasonable security measures and comply with schools' requests to delete student information.

FAQ M.4 recommends that, as a best practice, schools should consider providing parents notice of the third-party website and app operators to whom the schools provide consent for the collection and use of students' information. The FTC staff also suggests making the operators' direct notices concerning their information practices available to interested parents, such as by maintaining the notices on a website or providing a link to the notices at the beginning of the school year. The FTC staff revised FAQ M.4 to remove language explaining that making the operators' direct notices available to interested parents allows those parents to assess the operators' practices and "exercise their rights under COPPA—for example, to review the child's personal information."

FAQ M.5 provides guidance for schools considering whether to enter into an arrangement with an operator that will collect, use, or disclose students' personal information. The FTC staff recommends that a school ask the following questions, among others, as it seeks

---

[1] For example, in September 2014, California enacted the Student Online Personal Information Protection Act (SOPIPA), which goes into effect January 1, 2016. S.B. 1177, 2013-14 Reg. Sess. (Cal. 2014). In addition, the White House is working with federal lawmakers on legislation modeled after SOPIPA that would prevent companies from using student information for targeted advertising or to create marketing profiles. See Natasha Singer, "Bill Would Limit Use of Student Data," The New York Times, March 22, 2015, *available at* http://www.nytimes.com/2015/03/23/technology/bill-would-limit-use-of-student-data.html.

[2] Lesley Fair, "COPPA and Schools: Updated FAQs from the FTC Staff," FTC Business Center Blog, March 20, 2015, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/03/coppa-schools-updated-faqs-ftc-staff.

[3] For additional information on the FTC's COPPA enforcement, see Eye on Privacy, "COPPA Looms Large for Mobile Apps," February 2015, *available at* https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Feb2015/index.html#6.

[4] "Complying with COPPA: Frequently Asked Questions," *available at* https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[5] *See e.g.*, Oklahoma Statutes, Title 70, § 3-168; Colorado Revised Statutes § 22-2-309; Idaho Code § 33-133; Arizona Revised Statutes, § 15-1045.

[6] For additional information on SOPIPA and California's other student privacy laws, see Eye on Privacy, "California Enacts Landmark Student Privacy Laws," October 2014, *available at* https://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Oct2014/index.html#5.

Continued on page 6...

FTC Updates School-Related COPPA Guidance . . . *(continued from page 5)*

to understand how the operator will collect, use, and disclose the information:

- What types of personal information will the operator collect from students?
- How does the operator use this personal information?
- What measures does the operator take to protect the security, confidentiality, and integrity of the personal information that it collects?
- What are the operator's data retention and deletion policies for children's personal information?

FAQ M.5 notes that if the operator has not enabled the school to review and delete the personal information collected from its students, the school cannot consent on behalf of the parent. FAQ M.5 also explains that a school cannot consent to the collection of student information on behalf of a parent if the operator will use or share the information for commercial purposes not related to the provision of services requested by the school, such as online behavioral advertising or building user profiles for commercial purposes.

The FTC staff updated FAQ M.5 to remind schools that, under the Protection of Pupil Rights Amendment,[7] Local Educational Agencies (LEAs) "must adopt policies and must provide direct notification to parents at least annually regarding the specific or approximate dates of, and the rights of parents to opt their children out of participation in, activities involving the collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling that information (or otherwise providing the information to others for that purpose)."

Former FAQ M.6 posed a hypothetical example about an educator who wanted to register students for an online social network without parental consent. The FTC staff explained that it removed FAQ M.6 as part of its continued effort to streamline the FAQs because the topic addressed in FAQ M.6 is sufficiently covered in FAQs M.1 and M.2, which discuss when educational institutions can consent to a website or app's collection, use or disclosure of students' personal information, and when the operator of a website or app can rely on educational institutions to provide consent.

Guidance Regarding Online Test Providers

The FTC staff also recently clarified the applicability of COPPA to providers of online tests in a January 23, 2015, blog post.[8] In the post, the FTC staff responded to questions about whether the Partnership for Assessment of Readiness for College and Careers (PARCC) and the Smarter Balanced Assessment Consortium, two consortia of state educational agencies, are covered by COPPA. The FTC staff explained that the testing providers, like most educational institutions, are not covered by COPPA because they are not commercial "operators."[9] The blog post explained that, while the FTC staff encourages all types of entities to respect children's privacy, "the FTC's enforcement authority doesn't extend to information collection by state governments or most nonprofits." The post also noted that under the Family Educational Rights and Privacy Act (FERPA), "educational agencies and institutions have specific obligations to protect student privacy, including protecting personal information from children's education records from further disclosure or uses without the written consent of the parent, unless permitted to do so under FERPA."

The recent updates to the FTC staff's school-related COPPA guidance demonstrate the importance of adequately protecting the privacy of student information. Service providers, such as website and mobile app operators, working with educational institutions to collect student information should be cognizant of their own requirements under COPPA and other federal and state laws that protect student privacy, as well as the requirements and recommended best practices for the educational institutions.

---

[7] 20 U.S.C. § 1232h(c).

[8] Lesley Fair, "Testing, Testing: A Review Session on COPPA and Schools," FTC Business Center Blog, January 23, 2015, *available at* https://www.ftc.gov/news-events/blogs/business-blog/2015/01/testing-testing-review-session-coppa-schools.

[9] COPPA applies to individuals and entities that operate websites or online services for commercial purposes and collect or maintain personal information from users of such websites or services. *See* 15 U.S.C. §§ 6501(2), 6502.

Status Update on the EU Data Protection Regulation

Christopher Kuner
Senior Privacy Counsel, Brussels
ckuner@wsgr.com

Cédric Burton
Of Counsel, Brussels
cburton@wsgr.com

Laura De Boel
Associate, Brussels
ldeboel@wsgr.com

On June 15, 2015, the Ministers of Justice of all 28 European Union member states, sitting as the Council of the EU (Council), reached a crucial agreement for the future EU data protection legal framework. Much work still needs to be completed, but this is a major step forward in the adoption of the EU General Data Protection Regulation (Regulation).

The Regulation introduces important changes to EU data protection law that will have a significant impact on companies doing business in the EU. While the timing of final approval is still unknown, the fact that the Council has reached a general approach significantly increases the chances that the final text of the Regulation will be adopted in the foreseeable future. To learn more about the practical implications for businesses and how to prepare for the new legal framework, please join our webcast on July 15.

Where Do We Stand?

Under the EU legislative process, three institutions are involved in the enactment of new legislation: (1) the European Commission (the Commission—executive arm of the European Union); (2) the European Parliament (the Parliament—directly elected representatives from all 28 EU member states); and (3) the Council of the European Union (the Council—governmental representatives from EU member states).

The EU legislative process is highly complex, but can be summarized as follows: the Commission makes a proposal for legislation, which is reviewed and discussed by the Parliament and the Council. Both the Parliament and the Council negotiate the text on their own. Within each institution, amendments are proposed to the Commission's text in order to reach a common position. Once each institution has reached its position, the three institutions attempt to reach agreement on the final text of the legislation (i.e., the Trilogue).

Below we describe the main steps and current status of the Regulation.

1. January 2012: The EU Commission Proposal. The Regulation was proposed by the Commission in January 2012[1] to replace the 1995 EU Data Protection Directive. The text introduced important changes to EU data protection law, including stricter rules regarding the use of consent as a legal ground for data processing; strengthened individuals' rights; restrictions on profiling activities; and increased sanctions for data protection violations. The proposal provides for administrative fines of up to 2 percent of a company's annual worldwide turnover, or up to €1 million (whichever is more). It also introduces new requirements in EU data protection law, such as a data breach notification requirement; the obligation to conduct data protection impact assessments; the principles of data protection by design and by default; and the obligation to appoint data protection officers. One of the main benefits of the proposal is the introduction of a one-stop shop regulator for companies doing business in multiple EU member states, meaning that they would be subject only to the jurisdiction of the Data Protection Authority (DPA) of the member state in which they have their main establishment[2]

2. March 2014: The EU Parliament Amendments. The Parliament issued its first draft report on the proposal in early 2013.[3] This text was heavily debated in Parliament and triggered massive comments from stakeholders. After lengthy debates in different committees, the Parliament adopted its amendments to the Commission's proposal in March 2014.[4] The amendments are generally stricter than the Commission's proposal. For example, they further strengthen the rights of individuals, impose additional restrictions on profiling activities and increase fines for data protection violations to up to €100 million, or up to 5 percent of a company's annual worldwide turnover (whichever is greater).

3. June 2015: The EU Council's Amendments. In parallel to the negotiations in the Parliament, the Council has been meeting since 2012 to discuss amendments to the Commission's proposal. In June 2015, the Council reached an agreement on its text of the Regulation.[5] The Council's general approach makes a number of significant changes, such as removing some of the restrictions applicable to the use of consent as a legal ground for processing personal data and adding some flexibility for companies to process personal for new purposes. However, the Council also significantly weakened the one-stop shop mechanism by limiting it to important cross-border cases and providing a role in the decision making process for all DPAs involved, which is a set-back compared to the Commission's proposal.[6]

4. Present Status: Trilogue Negotiations. The three EU institutions have started their final negotiations, which should lead, ultimately, to the adoption of the Regulation. There is momentum now on which the EU institutions should build to reach a final agreement. However, while there is broad agreement

[1] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
[2] For a detailed analysis of the Commission's proposal, see https://www.wsgr.com/eudataregulation/pdf/kuner-020612.pdf.
[3] See the Draft Report of the Parliament's Committee on Civil Liberties, Justice, and Home Affairs (LIBE Committee), which is the lead committee with regard to the data protection reform, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-501.927%2b04%2bDOC%2bPDF%2bV0%2f%2fEN.
[4] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.
[5] http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf
[6] For a detailed analysis of the Council's text, see https://www.wsgr.com/eudataregulation/pdf/BNA-0615.pdf.

Continued on page 8...

Status Update on the EU Data Protection Regulation . . . *(continued from page 7)*

between the EU institutions on many of the core principles, the exact wording of the final text of the Regulation still remains unclear and will have to be agreed on as the result of a compromise via the Trilogue meetings.

The main challenge of the Trilogue will be to reconcile diverging or opposing views. The Parliament is seen as the most privacy-oriented institution in the EU, while the Council is usually quite business friendly. The text that results from these negotiations is often the outcome of intense negotiations and the result of significant trade-offs. It sometimes produces compromises that are difficult to apply or interpret in practice. It thus remains to be seen how the EU institutions will manage to reach an agreement and what the final text of the Regulation will look like.

The Trilogue meetings are informal, and it is difficult for stakeholders to know what happens during this final stage of the legislative process as it takes place behind closed doors. At the first Trilogue meeting, on June 24, 2015, a timetable for the upcoming meetings was agreed on[7], with the aim of adopting the Regulation by the end of 2015. The next meeting is scheduled to take place on July 14 and will deal with the provisions on international data transfers. The Trilogue will be led by the Luxembourg Presidency and, if no agreement is reached by the end of 2016, by the Dutch Presidency. Both countries have substantial experience in handling European matters, which allows for some optimism.

Conclusions

The European Union has made significant progress toward the adoption of a new EU data protection framework, but important work still remains. The Parliament's text that was adopted in March 2014 and the Council's text adopted in June 2015 are by no means the end of the story.

The Commission, Council, and Parliament are now in their final negotiations to reach an agreement. While there is some broad agreement on the core principles of the Regulation, the exact wording of the Regulation still remains unclear, and it will be the result of a compromise between the three EU institutions.

So far, all predictions have failed, but it now is reasonable to believe that a final text of the Regulation will be agreed on by the end of 2015 or during the spring of 2016. The Regulation will enter into force two years after its adoption, which means—at the earliest—end of 2017 or spring of 2018. Companies doing business in the EU or targeting EU individuals should start planning for the Regulation and assess how its new core principles will affect their business.

To keep up to date with the legislative developments concerning the Regulation, see our Wilson Sonsini Goodrich & Rosati's EU Data Protection Regulation Observatory at https://www.wsgr.com/eudataregulation/index.htm.

[7] The official timetable was not made public. However, an indicative timetable was published on the website of the Group of the European People's Party in the European Parliament: http://www.eppgroup.eu/news/Data-protection-reform-timetable.

New EU Trends: Cybersecurity and Breach Notification

Anna Pateraki
Associate, Brussels
apateraki@wsgr.com

Sarah Cadiot
Associate, Brussels
scadiot@wsgr.com

On June 29, 2015, the Council of the European Union (comprised of representatives of the 28 EU Member States) reached a political agreement with the European Parliament on the main principles of the draft Directive on Network and Information Security (NIS Directive) governing cybersecurity issues. The draft NIS Directive is an advanced piece of draft legislation in the EU that, once adopted, will likely concern a significant number of companies doing business in Europe. The final text is expected to be adopted sometime in late 2015, however the ultimate timing will depend on the political developments.[1] The draft NIS Directive is an advanced piece of draft legislation in the EU that, once adopted, will likely concern a significant number of companies doing business in Europe.[2] The final text is expected to be adopted sometime in late 2015, however the ultimate timing will depend on the political developments.

Background

The draft NIS Directive was proposed by the European Commission on February 7, 2013, and is undergoing the EU legislative process which is currently being finalized. It is part of the European Commission's broader Cybersecurity Strategy which defines core principles and policies for cybersecurity in Europe.[3] The Commission explains the need to propose a cybersecurity law by stating that:

> "Cybersecurity incidents or breaches can have a major impact on individual companies and on Europe's wider economy. [A] data breach could cost a company anything up to US$58 million, with [...] reputational damage, loss of customers and market share"[4]

The draft law would introduce the following aspects: (1) an incident notification requirement for companies; (2) an enforcement network comprised of national regulators and the European Commission; (3) regulatory investigations and audits; and (4) security requirements and standards.

What Industries Are Covered?

The draft NIS Directive would most likely affect the following types of companies:

- Critical infrastructure providers, such as companies from the financial, banking, energy, transport and health sectors; and
- A variety of Internet companies (e.g., domain names registries, e-commerce platforms, Internet payment services, social networks, search engines, cloud computing services, app stores).

While the initial Commission proposal included a detailed catalog of Internet industries that would be affected by the new breach notification requirements, the application of the NIS Directive on those industries has been heavily debated during the legislative process. Most likely, the NIS Directive would set out criteria based on which national law would determine what types of Internet companies would be covered.

In any event, once the NIS Directive has been adopted at the EU level, the EU Member States will have to transpose it into their own national law. It cannot be excluded that some national laws might go beyond the minimum requirements set out at the EU level and apply the cybersecurity rules to additional business sectors and/or set out additional requirements, which might lead to divergent cybersecurity laws in Europe.

Mandatory Notification of Cybersecurity Incidents

The draft NIS Directive would require a broad array of companies to notify cybersecurity incidents to national regulators. This would apply to incidents with a "significant impact" on the security of a company's core services. However, a simplified regime might be introduced regarding Internet companies, the details of which are yet to be finalized.

Alongside the breach notification obligation, the draft NIS Directive also provides minimum security requirements for network and information systems. While the draft NIS Directive sets out these minimum security requirements, EU Member States would not be prevented from adopting a higher level of security, which might have an impact on the types of incidents that would have to be reported at national level.

In addition, the regulator would have the power to inform the public directly about the cybersecurity incident or to require the company to do so. The draft NIS Directive does not describe in details the conditions of this mandatory notification regime, therefore leaving leeway on national law to set out further criteria. However, the draft NIS Directive mandates EU Member States to set out sanctions for non-compliance with the mandatory notification regime.

---

[1] See Council's press release http://www.consilium.europa.eu/en/press/press-releases/2015/06/29-network-information-security/.
[2] Proposal for a Directive concerning measures to ensure a high common level of Network and Information Security across the Union, COM(2013) 48 final (February 7, 2013).
[3] See http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
[4] See FAQ on the proposed Cybersecurity Directive, available at http://europa.eu/rapid/press-release_MEMO-13-71_en.htm (February 7, 2013).
[5] For more information see C. Kuner, A. Pateraki, *Eye On Privacy* newsletter, available at http://www.wsgr.com/publications/PDFSearch/eye-on-privacy/Nov2012/index.html.
[6] This is based on the implementation of the EU e-Privacy Directive into national law, Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications, available at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058.

Continued on page 10...

New EU Trends: Cybersecurity and Breach Notification . . . *(continued from page 9)*

The Breach Notification Landscape in Europe

The draft NIS Directive builds on the existing EU privacy rules but goes beyond them. Under the existing EU privacy rules, most EU countries do not have a general legal requirement for all sectors to notify data breaches to regulators, except in a limited number of countries.[5] Currently, most EU countries only have a sector-specific requirement for telecom providers and Internet Service Providers (ISPs) to notify security breaches to regulators and affected individuals.[6] However, this will change in the future with the forthcoming adoption of the draft EU General Data Protection Regulation which will impose a general data breach notification requirement in all EU Member States and for all sectors.[7]

Adding to this the upcoming breach notification requirement under the NIS Directive, companies will likely be faced with a number of different and potentially conflicting breach notification requirements in Europe. It remains to be seen what the exact area of overlap among the various notification requirements will be and how regulators and companies will work together to have those requirements coexist in practice.

---

[7] For more information, see the WSGR EU Data Protection Regulation Observatory, http://www.wsgr.com/eudataregulation.

President Obama Creates New Sanctions Regime to Combat Foreign Cyberthreats

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

Lawrence Perrone
Associate, Washington, D.C.
lperrone@wsgr.com

Katherine McCarthy
Associate, Washington, D.C.
kmccarthy@wsgr.com

On April 1, 2015, President Obama issued an executive order declaring "cyber-enabled malicious activities" a national emergency due to the "increasing prevalence and severity" of such attacks originating from or directed by persons outside the United States.[1] The executive order gives the Secretary of the Treasury, in consultation with the Attorney General and the Secretary of State, the power to impose economic sanctions on certain designated individuals and entities that have been directly or indirectly involved in malicious cyberattacks against U.S. networks, critical infrastructure, as well as those involving the theft of economic resources or personal and financial information, or the misappropriation of trade secrets.

Though the executive order did not contain a list of designated individuals, it does outline and provide a framework for the use of the Department of the Treasury's economic sanctions regime to combat significant cyberthreats. Any individuals or entities designated by the Treasury Department under the executive order will be subject to a travel ban and "blocked," meaning that any of their property or interests in the United States will be frozen, and U.S. persons may be prohibited from conducting business or otherwise transacting with that person and their property (hereinafter "blocked person"). The types of cyber-enabled activities, individuals, and entities targeted by the executive order are discussed below, along with the U.S. government's enforcement philosophy and key takeaways from this presidential action.

Cyber-Enabled Activities Targeted

The executive order authorizes the Department of the Treasury to impose sanctions on individuals and entities that engage in specific types of malicious cyber-enabled activities. To be subject to sanctions, the underlying cyber-enabled activity must meet a two-pronged standard. First, the cyber-enabled threat must be "reasonably likely to result in" or have "materially contributed to" a "significant threat to the national security, foreign policy, or economic health or financial stability of the United States."[2] Second, the designated individual or entity must be "responsible for or complicit in" or have engaged in at least one of the following categories of cyber-enabled conduct:

1. Harming or significantly compromising a computer or network of computers belonging to or supporting an entity in a critical infrastructure sector, or the provision of services by an entity in a critical infrastructure sector; [3]

2. Significantly disrupting computer or network availability;

3. Causing a significant misappropriation of economic materials including funds, trade secrets, personal information, or financial information for the purpose of commercial or competitive advantage or private financial gain;

4. The receipt or use of misappropriated trade secrets, knowing they have been misappropriated, for a commercial or competitive advantage or private financial gain or use by a commercial entity;

5. Materially assisting, sponsoring, or providing of financial, material, or technological support for, or goods or services in support of, any activity described in any of the aforementioned conduct or any person blocked under this Order;

6. To be owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person blocked under this order; or

7. Attempting any of the conduct listed above.

As is clear from this standard, the executive order does not target all malicious cyber-enabled activities originating outside the U.S. Rather, these sanctions will only target those malicious cyber-enabled activities that may have a significant threat to U.S. national security interests, foreign policy, or economic health and financial stability.

Relevant Sanctions

Section 1 of the executive order emphasizes that the administration is willing to impose severe financial sanctions against the perpetrators and supporters of malicious cyberattacks against the United States. While it is not yet clear how this executive order will be implemented, the regulatory regime will likely be similar to the counter-terrorism, counter-proliferation, and counter-narcotics sanctions already administered by the Department of the Treasury. As with those regimes, the sanctions to be imposed against malicious cyberattacks will be individual or entity-specific rather than against whole countries.

---

[1] Executive Order No. 13,694, 80 Fed. Reg. 18077 (Apr. 2, 2015).
[2] *Id.*
[3] Critical infrastructure sectors include energy, emergency services, financial services, healthcare, defense, transportation, information technology, food and agriculture, nuclear resources, water and wastewater systems, critical manufacturing, chemical, dams, and communications as well as the government facilities sector. See http://www.dhs.gov/critical-infrastructure-sectors.

Continued on page 12...

President Obama Creates New Sanctions Regime . . . *(continued from page 11)*

After designation, the blocked person will likely be added to the List of Specially Designated Nationals and Blocked Persons (SDN List) administered by the Department of the Treasury's Office of Foreign Assets Control (OFAC). U.S. persons are prohibited from conducting business or otherwise transacting with Blocked Persons. Those that do so may be subject to an investigation and/or enforcement action by OFAC. The civil penalties for violations range from $250,000 per violation or twice the value of the underlying transaction. Criminal penalties for willful violations can be as high as $1 million or 20 years imprisonment.

Enforcement Philosophy

In signing the executive order, the president stated that the United States was "giving notice to those who pose significant threats to our security or economy by damaging our critical infrastructure, disrupting or hijacking our computer networks, or stealing the trade secrets of American companies or the personal information of American citizens for profit."[4] The executive order serves as a new tool to battle malicious cyberattacks "that may be beyond the reach of our existing capabilities."[5]

Additionally, one of the critical goals of this new sanction regime is to remove the financial motivation underlying many cyberattacks. Lisa Monaco, Assistant to the President for Homeland Security and Counterterrorism, recently stated that "freezing assets of those subject to sanctions and making it more difficult to do business with U.S. entities . . . [will] remove a powerful economic motivation for committing these acts in the first place."[6] The executive order will provide the Secretary of the Treasury with the authority to punish those who use cyberattacks to threaten the United States and to deter those considering potential future attacks.

Though the authority granted by the executive order is broad, the Obama administration has stated that it will be utilized in a "targeted manner against the most significant cyberthreats we face."[7] The sanctions should be reserved for the "worst of the worst of malicious cyber actors."[8]

Key Takeaways

While the executive order provides the government with a powerful tool to address malicious cyber-enabled activities, the extent to which such measures will be effective in the overall deterrence of cyberattacks is not yet known. What is known, however, is that non-compliance with economic sanctions may result in costly investigations and enforcement penalties. To ensure compliance with economic sanctions, companies should adopt written policies and implement procedures to screen their customers, employees, and third-party business partners against the prohibited party lists maintained by the Departments of Commerce, State, and the Treasury, which includes the SDN List administered by OFAC. If a process is already in place, companies should confirm that their screening mechanism includes the most recent updates to prohibited party lists to ensure newly added entries based on the executive order are captured.

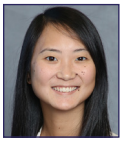
Additionally, companies should adopt policies and procedures designed to handle cyber incidents including the adoption of best practices related to the detection, categorization, containment, and remediation of cyber events. Companies that detect malicious cyber-enabled activities may consider reporting such activities to the U.S. government (and may be required to do so in some instances). Such information sharing may result in the addition of certain individuals or entities to a prohibited party list on the authority provided in this executive order. In fact, the administration encourages such information sharing as evidenced by President Obama's February 12, 2015, executive order designed to "promote sharing of cybersecurity threat information within the private sector and between the private sector and government."[9]

The bottom line is that companies should be considering both cyber incident response and economic sanctions from a compliance perspective in order to confront the effect of and minimize the legal risk presented by cyberattacks.

---

[4] The White House Blog, "Our Latest Tool to Combat Cyber Attacks: What You Need to Know" (April 1, 2015) (*quoting* President Barack Obama).
[5] *Id.*
[6] Expanding Our Ability to Combat Cyber Threats, National Security Council (April 1, 2015).
[7] Fact Sheet, The White House Office of the Press Secretary, "Executive Order Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities" (April 1, 2015).
[8] *See Supra*, fn 4.
[9] Fact Sheet, The White House Office of the Press Secretary, "Executive Order Promoting Private Sector Cybersecurity Information Sharing" (February 12, 2015).

Privacy Laws in the Digital Age—A Push for Increased Protections



Dylan Savage
Associate, New York
dsavage@wsgr.com

Whitney Costin
Associate, New York
wcostin@wsgr.com

Protection of highly sensitive personal information is a growing concern for most Americans in the ever-increasing digital age, especially in the wake of large-scale data breaches from leading retail brands and healthcare providers. Although protections currently exist to counteract unwanted dissemination of private information, as well as rules mandating notification when such unwanted dissemination occurs, this growing concern has prompted the White House and Congress to take steps toward increasing protections in the context of privacy laws.

On January 12, 2015, President Obama delivered remarks before the Federal Trade Commission in which he announced "new steps to protect the identities and privacy of the American people," including the Consumer Privacy Bill of Rights, the Personal Data Notification and Protection Act, and the Student Digital Privacy Act.[1] Each of these proposals would strengthen protections for either consumers or students and would create a uniform standard for privacy laws to replace piecemeal legislation enacted on a state-by-state basis. Although none of these proposed bills have been enacted into law, and neither the Consumer Privacy Bill of Rights nor the Student Digital Privacy Act have even been formally introduced to Congress, all have drawn wide attention and prompted a debate on how far privacy laws should extend.

Consumer Privacy Bill of Rights

On February 23, 2012, the White House published a whitepaper detailing President Obama's plan for a universal framework implementing certain data privacy standards for corporations which collect and use individuals' personal data. Following more than two years of consultation with industry participants, on February 27, 2015, the White House released a "discussion draft" of the Consumer Privacy Bill of Rights Act (CPBR), which is intended to be the cornerstone of the administration's privacy framework.[2] The CPBR is intended to "establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders." It would preempt any state or local regulations to the extent that they impose requirements on personal data processing.

In particular, the CPBR is aimed at increasing both transparency in corporate data practices and individual control over the storage and use of personal data that companies collect and retain. With respect to transparency, a "covered entity" is required to provide clear and concise notice to individuals about a company's privacy and security practices. Among other things, the notice must include information about the types of personal data processed by the covered entity, the purposes for which that data is used and to whom it will be disclosed, the specific measures taken to secure personal data, and the persons whom individuals may contact regarding the covered entity's data processing.

Under the CPBR, individuals must also be given means to control the processing of their personal data that are reasonable in light of the potential privacy risks and the particular context. If a person withdraws consent for a covered entity to collect or maintain his or her personal data, the company must delete or de-identify the data within a "reasonable" time frame. Any covered entity which does not "process[] personal data in a manner that is reasonable in light of context" must conduct a privacy risk analysis and provide individuals with heightened transparency and a mechanism by which individuals may choose to reduce such privacy risk. An exemption from the heightened notice and control requirements is provided for companies that are supervised by FTC-approved Privacy Review Boards.

In addition, the CPBR requires the focused collection and responsible use of personal data, and covered entities must conduct a risk analysis of threats that could result in authorized disclosure of individuals' information. Companies must also undertake certain internal measures to ensure compliance with the obligations of the CPBR, such as providing employee training and integrating consideration for privacy and data protections into the company's systems.

Violations of the CPBR are treated as an unfair or deceptive act or practice in violation of Section 5 of the Federal Trade Commission Act, and the FTC may levy penalties of up to $25 million. Notably, the CPBR includes a safe harbor provision for covered entities that develop a code of conduct for the processing of personal data. The codes of conduct must undergo a public comment process and are subject to approval by the FTC, which turns on whether the code of conduct provides protections for personal data that are equal than or greater to those otherwise provided in the CPBR.

Reaction to the bill has been mixed. Among the bill's biggest supporters is Microsoft, which lauded the CPBR as a "welcome development that [it] hope[s] will kick-start a much-needed conversation about how to protect people's personal information."[3] The FTC, however, espoused concerns that the draft bill fails to provide the "strong and enforceable protections needed to safeguard [consumers'] privacy."[4] The FTC is in accord with this opinion, and the sentiment is also echoed by Democratic legislators, who fear that the bill falls short and believe that the emphasis on self-regulation is a flawed solution.

To that end, a coalition of privacy groups, including the Center for Digital Democracy, drafted a letter criticizing both the development of the CPBR—during which the White House

[1] The full text of President Obama's remarks before the Federal Trade Commission can be found here: http://www.gpo.gov/fdsys/pkg/DCPD-201500022/pdf/DCPD-201500022.pdf.
[2] The full text of the proposed legislation can be found here: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[3] The full text of Microsoft's statement can be found here: http://blogs.microsoft.com/on-the-issues/2015/02/27/white-house-proposal-elevates-privacy-transparency-discussion/.
[4] Andrea Peterson, "The White House's draft of a consumer privacy bill is out – and even the FTC is worried," *The Washington Post*, Feb. 27, 2015, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2015/02/27/the-white-houses-draft-of-a-consumer-privacy-bill-is-out-and-even-the-ftc-is-worried/.

Continued on page 14...

Privacy Laws in the Digital Age . . . *(continued from page 13)*

allegedly shut out many privacy watchdog organizations from the consultation process—and the substance of the draft bill. The coalition argues that the draft bill does not vest enough power in the FTC and places too much discretion in the hands of companies through the many provisions aimed at self-regulation. Furthermore, the coalition is concerned that the bill may preempt stronger state legislation and could ultimately weaken privacy protections for many citizens.

Similarly critical are those in the tech industry, but for opposite reasons. The Internet Association is worried that the bill is "needlessly imprecise,"[5] and the Consumer Electronics Association fears that it could be harmful to innovation. Differences aside, both the bill's supporters and its detractors can agree that the legislation is not likely to pass in its current form, and the main value of the discussion draft is to engender a more robust dialogue around the privacy issues that are relevant in today's digital age.

Personal Data Notification and Protection Act

As the rate of cyberattacks continues to rise, so do concerns from the public regarding the security of highly sensitive personal information in the custody of businesses. Although most states have enacted variations on legislation that mandate notification to individuals in the event of a breach or potential breach of personal, sensitive information,[6] to date there is no uniform federal standard with which businesses are required to comply.

The Personal Data Notification and Protection Act, promoted by the White House and introduced to the U.S. House of Representatives on March 26, 2015, by Rep. James R. Langevin, would create a uniform notification standard with which businesses holding records for more than 10,000 individuals within any 12-month period must comply in the event "sensitive personally identifiable information" has been breached or "reasonably believed" to have been breached.[7] Businesses would be required to notify customers within 30 days of discovering the breach, unless the Federal Trade Commission determined there would be no reasonable risk to customers or disclosure would be preempted by national security or other specifically enumerated concerns.[8] The legislation would also criminalize illicit overseas identity trade. The bill, H.R. 1704, is currently before the U.S. House of Representatives and has been referred to the Committee on Energy and Commerce and the Committee on the Judiciary for comment.

Critics of the Personal Data Notification and Protection Act, such as various privacy advocacy groups, see this new legislation as weak and a barrier to effective and more extensive legislation already passed in a variety of states.[9] After all, weaker federal legislation, if passed, would pre-empt state legislation and thus eliminate rights of citizens of states whose strong privacy standards currently provide additional protections not encompassed in H.R. 1704. Advocates, such as many financial and retail groups, feel that a uniform information-sharing policy would not only benefit businesses' ability to comply with notification laws, but would also facilitate collaboration between industry and government to eradicate or lessen the threat of cybercriminals.

Student Digital Privacy Act

Following the wave of proposed legislation marked to ease general privacy concerns, the Student Digital Privacy Act aims to alleviate concerns that the private information of students in kindergarten through 12th-grade is being used commercially. Specifically, this proposed legislation would require educational institutions to use data collected on students in the classroom solely for educational purposes and would ban the sale or use of student data to third parties for unrelated, non-educational purposes, including targeted advertising and marketing. Although legislation currently exists to limit the sale or use of students' private educational records, the fact that this legislation has not been updated in four decades has many concerned and has prompted calls from both the White House and many in Congress for an active reform of such protective legislation.

The bill, however, is already off to a rocky start. Set to introduce the bill on Monday, March 23, 2015, Reps. Jared Polis and Luke Messer delayed introduction of the bill to smooth out concerns voiced by advocacy groups. The Student Digital Privacy Act has garnered resistance from advocates on both sides of the debate, including those who favor self-regulation and those who call for stronger protections or consent requirements, such as those mandated in California under the Student Online Personal Information Protection Act. Despite some resistance, however, at least 75 companies have signed the Student Privacy Pledge, a promise, among other things, not to sell student information or behaviorally target students and to only use data for certain authorized purposes. Although draft proposals of the bill have been said to be circulating in Washington, D.C., no formal proposed bill has been released to the public or has been formally proposed in the U.S. House of Representatives or U.S. Senate.

---

[5] The full text of The Internet Association's statement can be found here: http://internetassociation.org/022715privacy/.

[6] Reference to state-by-state privacy legislation requiring notification following security breaches of personally identifiable information can be found here: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Currently, Alabama, New Mexico, and South Dakota are the only states that have not enacted privacy breach notification legislation.

[7] The bill as introduced to the 114th Congress can be found here: http://www.gpo.gov/fdsys/pkg/BILLS-114hr1704ih/pdf/BILLS-114hr1704ih.pdf.

[8] The Federal Trade Commission could delay notification time upon determining a delay would prevent further breaches or would be necessary to determine the scope of the breach.

[9] California and Connecticut, for example, have five-day notification requirements as compared with the proposed 30-day notification requirements in H.R. 1704.

Canadian Anti-Spam Legislation Shows Its Teeth with First Enforcement Actions

Jonathan Adams
Associate, San Francisco
jadams@wsgr.com

The Canadian Anti-Spam Legislation (CASL) is now showing that it has strong teeth. CASL requires companies operating in Canada to obtain affirmative opt-in consent prior to sending commercial electronic messages (CEMs), such as emails or text messages, within Canada. In addition, any CEM sent must contain certain identification information and provide recipients with a means of opting out or unsubscribing from future messages. These requirements were enacted in December 2010, and CASL provided a grace period that ended on July 1, 2014. Now that CASL is subject to enforcement, the Canadian Radio-television and Telecommunications Commission (CRTC), which is charged with enforcing CASL, has announced two enforcement actions that should place organizations operating in Canada on notice that violations of the law may result in significant penalties.

In the first announced action, on March 5, 2015, the CRTC's chief compliance and enforcement officer issued a Notice of Violation and a CA$1.1 million penalty to a Quebec-based company, Compu-Finder, for four violations of CASL. These violations, which persisted from July 2014 to September 2014, allegedly included sending unsolicited email (including business-to-business messages) and failing to include a functioning unsubscribe mechanism. The CRTC also alleged that Compu-Finder "scoured" websites to obtain email addresses, and that Compu-Finder's actions were the source of 26 percent of the spam complaints the CRTC received in the period Compu-Finder was sending the unsolicited emails. Under the terms of the Notice of Violation, Compu-Finder had thirty days to file written representations to the CRTC to contest the charges or to pay the penalty.

In the second action, the CRTC announced on March 25, 2015, that online dating website operator Plentyoffish Media Inc. entered into an undertaking (essentially, a binding promise that may be entered into before or after a Notice of Violation is issued) and paid CA$48,000 to the CRTC as an "administrative monetary penalty" for an alleged violation of CASL. In addition, Plentyoffish was required to develop and implement a program to ensure that its marketing activities comply with CASL, including staff training and education and the development of relevant corporate policies and procedures. The CRTC commenced its investigation of Plentyoffish following complaints that commercial emails Plentyoffish sent to its registered users from July 2014 through October 2014 did not have an unsubscribe mechanism that was clearly and prominently visible and readily performable. In comments, the CRTC noted the importance organizations must place on ensuring that the content of their CEMs meet CASL requirements. Notably, the Plentyoffish enforcement led to an undertaking, and it appears that no Notice of Violation will follow, likely because Plentyoffish took prompt steps to cease its CASL non-compliance by updating its unsubscribe mechanism to comply with law.

These cases did not involve the maximum administrative monetary penalties that the CRTC may seek under CASL: such penalties reach CA$10 million for organizations and CA$1 million for individuals. Other enforcement mechanisms available to the CRTC, beyond Notices of Violation and undertakings with administrative monetary penalties, include warning letters, preservation demands, production notices, and restraining orders. In addition, commencing July 1, 2017, individuals will have a private right of action under CASL. Individuals will be permitted to seek court orders awarding actual and statutory damages resulting from CASL violations; statutory damages may reach as high as CA$1 million for each day on which a CASL violation occurred. Note, however, that no private litigant may receive statutory damages for CASL violations where the defendant entity has received a Notice of Violation from, or has entered into an undertaking with, the CRTC. Thus, once the private right of action becomes available in mid-2017, entities that have failed to comply with CASL will have ample reason to cooperate with the CRTC if cooperation may lead to reduced remediation costs. Nevertheless, avoiding CASL violations should be a priority for all organizations conducting business in Canada. As a result, organizations should: (i) review their CEM mechanisms for CASL compliance, ensuring appropriate unsubscribe mechanisms are in place and that recipient consent has been obtained; (ii) ensure the implementation of robust CASL policies and procedures; and (iii) carry out CASL training in connection with general marketing compliance training.

Upcoming Privacy & Data Protection Events

Webcast: An Update on the EU Data Protection Regulation
July 15, 2015, 9:30 a.m. – 10:30 a.m. PDT

As the EU moves closer to adopting new data protection legislation, companies doing business in the EU should start assessing how the changes will affect their activities. This webcast will provide an update on where things stand, as well as practical advice on how to prepare for the new EU data protection framework. WSGR attorneys will provide a summary of the debate surrounding the Regulation in the EU and discuss what we can expect over the next few months. They will analyze the implications for businesses and provide practical advice on how to prepare for the new legal framework.

Click here for registration information and additional event details.

The Future of Privacy in a Connected World: A Cross-Border Conversation
September 16, 2015

A insightful panel discussion with key policymakers in the United States and the European Union on global privacy and data protection speaking on critical privacy issues in the U.S. and EU, including: privacy regulation around big data, the Internet of Things, and other developments in cutting-edge digital communications; recent changes in online privacy regulation and self-regulation; the latest news on the EU data protection regulation, and implications for U.S. companies; and the evolving legal climate around global privacy enforcement.

More program details and registration information to be announced soon.

Other Industry Events

IAPP Privacy Academy and CSA Congress
September 29 - October 1, Las Vegas
https://privacyassociation.org/conference/privacy-security-risk-2015

2015 International Privacy Conference
October 26-29, Amsterdam
http://www.apc2015.net/content/amsterdam-privacy-week

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