Skadden

PRIVACY & CYBERSECURITY UPDATE

JULY 2014

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 5, or your regular Skadden contact.

TREASURY SECRETARY CALLS FOR INCREASED FOCUS ON CYBERSECURITY

On July 16, 2014, U.S. Secretary of the Treasury Jack Lew delivered remarks at the 2014 Delivering Alpha Conference, urging Congress to pass cyberlegislation and encouraging companies to more actively share information regarding cyberthreats. Lew's speech follows a trend of increased government attention to cyberrisks in the financial sector. As we reported in our April 2014 *Privacy & Cybersecurity Update*, the SEC hosted a roundtable in March to discuss disclosure requirements related to cyber-attacks.

Lew began by establishing the serious nature of cyberthreats by providing an account of recent incidents, from the massive data breach at Target to the false announcement of an attack on the White House through a hack of The Associated Press' Twitter account that drove the Dow Jones industrial average down by more than 100 points in three minutes. Lew stressed that although successful attacks to the financial system represent an economic and national security threat, the dangers posed by cyberthreats are not unique to financial institutions. The risk starts with vendors and suppliers, affects the energy and telecommunications industries, and can endanger the nation's physical infrastructure.

Given the widespread vulnerability to cyber-intrusion, companies' precautionary activities have been vastly inconsistent. While some banks already are spending considerable amounts on cybersecurity, other institutions are just beginning to develop their defenses. Lew urged all companies to remedy this weakness by adopting the NIST cybersecurity framework issued in February 2014,[1] involving all levels of management in the process through better internal communication of cyberrisk considerations, and — most importantly — engaging in greater collaboration with government agencies and other firms. According to Lew, such information sharing will allow for the development of best practices. In addition, awareness of "specific attacks and attackers" will help companies reduce susceptibility to further breaches and will allow the government to fulfill its "public responsibility to prosecute cyber criminals [and] hold state-sponsored attackers accountable." Lew recognized the hesitation to disclose incidents due to potential reputational harm, but insisted that "sharing information is far too essential" to let such concerns stifle information flow.

In a brief but climactic portion of his speech, Lew declared that "it is time for Congress to pass cyber legislation." The executive branch already has made cybersecurity a priority, creating a Financial Sector Cyber Intelligence Group dedicated to the analysis of law enforcement and intelligence reports and the delivery of information bulletins that financial institutions can use to enhance protection, and regularly discussing cybersecurity in bilateral meetings with foreign leaders. According to Lew, the law has not yet caught up. Lamenting the current legal regime's inability to adequately "defend the public from digital threats," he called for laws with "clear rules" that facilitate responsible collaboration through "important liability protection." Any legislation should aim to make companies feel safer in sharing information about cyberthreats, but should not provide immunity for "reckless, negligent or harmful behavior."

Although Lew did not endorse any specific legislation, he positively acknowledged the "various bills that are developing in Congress." The Cyber Information Sharing

[1] Available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

Act (CISA) is the most prominent of these bills. The newly Senate-drafted version of the bill, which has twice failed to pass both chambers in previous incarnations, would provide broad immunities to companies that share threat data with "any other entity or the federal government" for cybersecurity purposes. The bill, like its predecessors, has faced opposition for its supposed failure to adequately protect citizens' privacy. This is perhaps one of the reasons Lew refrained from discussing particular legislation, but instead commented that any legislation should "protect individual privacy and civil liberties, which are so essential to making the United States a free and open society."

Notably absent from Lew's remarks was any discussion of public disclosure. While the public is concerned with cybersecurity legislation's impact on privacy, companies expressed concerns related to more-than-boilerplate public disclosures of material incidents and cyberrisks in a March SEC roundtable. Lew's comments indicate that the interconnected economy, and resultant high stakes of potential systemic harms of cyber-attacks, make collaboration and information sharing between the private sector and the government (not the public) the top priority — not for investors' sake, but for protection of the nation's overall economic stability and national security.

Return to Table of Contents

NEW REQUIREMENTS FOR 'CLEARED INTELLIGENCE' CONTRACTORS

The Intelligence Authorization Act for Fiscal Year 2014 (the Act), which authorizes intelligence appropriations for the year, contains new requirements for cleared intelligence contractors to report cybersecurity breaches.[2] The comprehensive law, signed on July 7, addresses general appropriations matters and assigns various responsibilities to different elements of the intelligence community. Particularly salient for cybersecurity is Section 325 of the Act, a provision that describes mandatory "Reports to the Intelligence Community on Penetrations of Networks and Information Systems of Certain Contractors."

Section 325 requires the Director of National Intelligence (DNI) to create procedures that will in turn require cleared intelligence contractors to report breaches of "covered" networks and information systems. The Act defines a "covered network" to be a "network or information system of a cleared intelligence contractor that contains or processes information created by or for an element of the intelligence community," though only if that network fits certain criteria to be promulgated as part of the reporting procedures. In addition, the Act leaves to the DNI's discretion which element or elements of the intelligence community will handle incoming breach reports.

The Act does prescribe a baseline set of information that a breach report must contain. When an intelligence contractor discovers a breach of a covered network, the contractor must report a description of the method used to penetrate the system; a sample of the malicious software, if it has been discovered and isolated; and a summary of any information created by the element of the intelligence community to which the contractor is reporting that has been compromised or potentially compromised by the breach. The Act requires the contractor to make the report "rapidly" but assigns no specific time frame.

After a contractor reports a breach, intelligence community personnel can obtain access to the contractor's equipment or information pursuant to Section 325(c)(2). Any such access must be for the limited purpose of determining whether and what information may have been exfiltrated. The procedures for providing such access must reasonably protect trade secrets, commercial or financial information, and personally identifying information. Information derived through the new reporting procedures can be disseminated outside of the intelligence community if a contractor gives approval, or may be given without approval to Congress for oversight purposes or to law enforcement in order to investigate the cybersecurity incident in question.

---

[2] Intelligence Authorization Act for Fiscal Year 2014, Pub. L. No. 113-126, (July 7, 2014), *available at* https://beta.congress.gov/113/bills/s1681/BILLS-113s1681enr.pdf.

As many cleared intelligence contractors are also cleared defense contractors, Section 325(e) requires the DNI to confer with the secretary of Defense to create joint reporting procedures, so that a contractor who meets both definitions can submit one report that simultaneously satisfies both the Intelligence Authorization Act and the National Defense Authorization Act of 2013 (NDAA), which mandates similar reporting requirements for defense contractors.[3]

PRACTICE POINTS

The DNI has 90 days from the Act's enactment to create specific reporting procedures, at which time the Act's reporting requirements will go into effect. Note, however, that the parallel rulemaking required under the NDAA has been delayed past the statutory 90-day deadline, and that the Act's deadline may slip as well. Alternatively, if the Department of Defense meets its extended deadline next month for the NDAA cybersecurity rulemaking, the DNI procedures may be influenced by the defense reporting requirements. Once the reporting requirements are put in place, cleared contractors will be able to determine which networks are covered networks and which elements of the intelligence community will require breach notification. Contractors operating covered networks should be aware that access to information transiting those networks may now be granted to law enforcement without their consent after a breach.

More generally, private companies doing business with the federal government, even those outside the defense and intelligence sectors, should be aware that the procedures required under the Act and the NDAA are part of an ongoing trend toward strengthening federal procurement requirements regarding contractor and vendor cybersecurity. The Consolidated Appropriations Act of 2014 included a supply chain-related provision requiring the Departments of Justice and Commerce, the National Science Foundation, and National Aeronautics and Space Administration to review their supply chain cybersecurity risk. Executive Order 13636 directed that DOD and the General Services Administration make recommendations to the president on the feasibility, security benefits and relative merits of incorporating security standards into acquisition planning and contract administration. Government contractors can expect to face increasing cybersecurity scrutiny in the months and years to come.

Return to Table of Contents

FTC CLARIFIES VERIFIABLE PARENTAL CONSENT METHODS UNDER COPPA

On July 16, 2014, the Federal Trade Commission (FTC) updated a section of Frequently Asked Questions (FAQs) related to obtaining verifiable parental consent under the Children's Online Privacy Protection Act (COPPA).[4] The latest in a series of updates, the FAQ clarifies and expands methods of obtaining consent available to website operators and mobile app developers, and provides entirely new guidance regarding the liability of third-party platforms.

HISTORY OF COPPA

COPPA was first enacted in 1998 to regulate the online collection of personal information of children under 13 years of age. After initiating a review in 2010 to ensure that the Act reflects evolving uses of the Internet, such as increased mobile and social networking use, the FTC issued a new COPPA Rule in December 2012 and gave companies until July 1, 2013, to comply.[5] The updated Rule expanded the types of personal information covered, extended liability

[3] National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, (Jan. 2, 2013), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-112publ239/pdf/PLAW-112publ239.pdf.
[4] Lesley Fair, *COPPAediting*, FTC Bus. Ctr. Blog (July 16, 2014, 2:02 PM), http://www.business.ftc.gov/blog/2014/07/coppaediting.
[5] Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information By Amending Childrens Online Privacy Protection Rule (Dec. 19, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over.

to information-collecting third parties such as plug-ins and advertising networks, and added a number of new parental notice and consent requirements.

These changes caused anxiety among app developers and the online third-party ecosystem. There was significant confusion over areas of the new rule, such as what constitutes "actual knowledge" that an advertising network is receiving data from a children's site and what satisfies the verifiable parental consent requirement. This not only increases the risk and cost of compliance, but COPPA violations bear extremely stiff penalties — up to $16,000 per instance of violation. Amidst concern that COPPA has stifled innovation of online content for children, and would further stifle the development of app and mobile economies under the new rule, online industry and business organizations sought a six-month extension of the effective date for the new rule. Instead of postponing the effective date, the FTC proceeded to issue a series of updates to the FAQs to clarify and guide operators in compliance. The most recent update is the third in this series, following updates that clarified the "actual knowledge" standard and that provided guidance for implementing COPPA in schools.

VERIFIABLE PARENTAL CONSENT

COPPA requires that operators give notice to parents and receive their consent before collecting personal information from children under 13 years of age. The acceptable methods of obtaining this consent and to whom these standards apply have been persistently confusing and created expensive compliance issues. In addition to the general compliance costs associated with COPPA, developers have complained of facing the supplemental cost of educating parents about their responsibilities as fiduciaries of their children's data.

The FTC partially ameliorated this confusion by including a provision in the rule that allows operators to submit suggested new methods for FTC approval to accommodate developing technology. Since 2013, when the updated COPPA took effect, the FTC has reviewed three applications for new methods of obtaining verified parental consent, including one to use the type of knowledge-based authentication used by financial institutions and credit bureaus (which was approved). Although this case-by-case approach provided some clarification, the new amendments provide much needed, wide-ranging guidance.

CURRENT AMENDMENTS

The first amendment incorporates and expands upon knowledge-based authentication. Whereas the previous version of this FAQ maintained that operators could not use a credit card or debit card number as a form of verifiable parental consent unless the number was used in connection with a monetary transaction, the updated FAQ allows such use as the credit card is combined with other safeguards that are "reasonably calculated, in light of available technology, to ensure that the parent providing consent is the child's parent." The FTC uses knowledge-based authentication to illustrate such an adequate alternative.

The second amendment confirms that an app developer may use third parties, such as app stores, to obtain parental consent on its behalf. This does not remove the developer's burden entirely. Operators still must ensure that a third party's verification methods meet COPPA requirements, and must provide parents with direct notice of their app's information collection practices before consent is provided.

Finally, the FTC added an entirely new FAQ directed at app stores and other third-party platforms. The new FAQ notes that an app store will not be liable for, and has no duty to investigate, the privacy practices of app developers because the app store is not an "operator" under COPPA so long as it merely provides a verifiable consent mechanism for app developers to use. The FAQ warns app stores that they may still face liability under Section 5 of the FTC Act if, for example, they misrepresent the level of oversight they provide for the apps on their platforms.

IMPLICATIONS

These changes "reaffirm the FTC's longstanding position that the agency's list of approved verifiable parental consent mechanisms is not exhaustive." The updated FAQs provide specificity and clarity that should reduce some of the burden on developers caused by uncertainty. The impact of this guidance is limited by its nonbinding nature; the FAQs do not obligate the FTC's enforcement actions in any way, but merely "offer an FTC staff take on practical issues." Nevertheless, the lessened confusion may lead to greater investment in children's apps and easier compliance by small businesses. The newly outlined liability regime for third parties additionally allows for the development of multiple platform consent mechanisms, whether by enterprising software developers or app stores themselves.

Web and app developers, advertisers and third-party platforms should continue to pay close attention to these and any future interpretive guidance related to COPPA. Impending FTC crackdowns, an increasing public interest in online privacy, and ever-growing data collection abilities and dependency suggest that such regulations are not going anywhere.

Return to Table of Contents

SMALL RETAILER FINED FOR FAILING TO PROVIDE DATA BREACH NOTIFICATION

Companies often assume that state attorneys general are concerned only with data breach notification in the case of large-scale cyber-incidents. However, a recent action by the Vermont attorney general revealed that this is not the case. The Vermont AG fined Shelburne Country Store in Shelburne, Vermont, $3,000 for failing to inform approximately 700 Internet buyers of a security breach of their credit card information. The store's website was hacked in late 2013 and, although they promptly remediated the problem, they failed to notify consumers until they were contacted by the AG's office. Under Vermont's Security Breach Notice Act, businesses are required to send the attorney general a confidential notice within 14 business days of discovery of a data breach. The business also must notify consumers in the most expedient time possible, but no later than 45 days. According to Vermont Attorney General William Sorrell, "we will not accept the excuse that a business did not know of its obligations to report a breach." The AG's action serves as an important reminder that companies must take their data breach notification obligations seriously, even in cases where they have remediated the breach.

Return to Table of Contents

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000