Skadden

PRIVACY & CYBERSECURITY UPDATE

AUGUST 2014

CONTENTS (click on the titles below to view articles)

NIST ANNOUNCES OCTOBER WORKSHOP AND RELEASES FRAMEWORK UPDATE

OCTOBER WORKSHOP

As directed by President Obama's Executive Order 13636, the National Institute of Standards and Technology (NIST) released its Framework for Improving Critical Infrastructure Cybersecurity (the Framework) in February 2014. The Framework does not require specific activities, but rather — as its title implies — provides a Framework for critical infrastructure companies, such as those in the energy sector, to assess and establish cybersecurity policies and procedures in order to reduce the cyber risk those entities face.

When the Framework was released, the NIST stressed that there would be an iterative process to improve and update the Framework in response to changing realities and input from a variety of stakeholders. Indeed, the Roadmap that accompanied the Framework stated:

> The Framework was intended to be a "living document," ... that will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."

To that end, the NIST is holding a fact-gathering workshop on the Framework on October 29 and 30.[1] The workshop will he hosted by the Florida Center for Cybersecurity, a state-funded entity located at the University of South Florida in Tampa.

The purpose of the workshop is to allow the NIST to gather information from stakeholders as to their awareness of and experiences with implementing (or considering implementing) the Framework. Such stakeholders include critical infrastructure owners and operators of all sizes, as well as cybersecurity staff and individuals who have operational, managerial and policy experience and responsibilities for cybersecurity. In addition, the NIST will solicit input from professional associations, government agencies and standards development organizations; industry and consumer groups; and solution providers and other stakeholders. The workshop is just the latest step in the NIST's ongoing efforts to raise awareness and encourage use of the Framework among stakeholders and to solicit feedback.

The NIST has said that prior to the workshop, it plans to issue a Request for Information. Responses to the RFI will be shared publicly.

FRAMEWORK UPDATE

Along with its announcement of the October workshop, the NIST released an update of the Framework that summarized progress that has been made to achieve those areas identified in the Framework Roadmap as requiring additional input and development, specifically where "the needs of Critical Infrastructure owners and operators extend

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.

[1] For details see http://www.nist.gov/cyberframework/6th-cybersecurity-framework-workshop-october-29-30-2014.cfm.

beyond those existing standards, guidelines, and practices." The update describes the steps that the NIST successfully has taken in the last six months, which include:

- Strengthened its collaboration with critical infrastructure owners and operators, industry leaders, government partners and other stakeholders. The goal of these interactions included raising awareness about the Framework and its intent, assisting sectors developing sector-specific implementation guides with their government partners and gaining feedback from users about their experiences — both positive and negative — with the Framework so that it can be improved in the future. The meetings have included discussions with regulatory agencies, sessions focused on the needs of small and medium sized businesses, broad-based industry-wide sessions, and meetings hosted by the Department of Homeland Security C3 Voluntary Program.
- The NIST recently released a Cybersecurity Framework Reference Tool[2] to assist companies in navigating the Framework and its standards, guidelines and best practices. Through this tool, users can browse the Framework core by functions, categories, subcategories and informative references; search for specific words; and export the data to various file types.
- In the area of authentication, the NIST has worked with the National Strategy for Trusted Identities in Cyberspace and partnered with the Identity Ecosystem Steering Group (IDESG) to support the development of better identity and authentication solutions. For example, the IDESG has agreed on a series of components for the Identity Ecosystem Framework and currently is crafting these components in anticipation of launching a self-assessment and self-attestation program early in 2015 with a more comprehensive program the following year.
- Developing a draft special publication that focuses on information sharing and coordination within the incident response life cycle. The publication will provide guidance on the safe and effective sharing of information in support of cross-organization incident response, an area of great interest and concern to many companies. A draft release of the publication is planned for Fall 2014.
- The NIST continues to work with the public and private sector on "conformity assessment" (*i.e.*, ways that industry could demonstrated conformity to a given Framework profile).
- Exploring how big data can be used to understand complex infrastructures and design security programs.
- Engaging the international community on the Framework by discussing the U.S. approach with multiple foreign governments and regional representatives including organizations throughout the world, including the United Kingdom Japan, Israel, Germany and Australia.
- Working with industry experts on supply chain risk management, a key are of concern for many in the industry. This includes promoting the mapping of relevant standards, best practices and guidelines to the Framework core and identifying key challenges and strategies to supply chain risk management to enable more effective Framework implementation.

Return to Table of Contents

INSURANCE COMPANY SUCCEEDS IN CYBERSECURITY LITIGATION

A growing and critical area of privacy and cybersecurity litigation involves the obligation of insurance companies to cover a company's losses under traditional commercial general liability policies. A recent decision by a federal district court in the state of Washington held that, on the facts before it, the insurance company had no such obligation.

National Union Fire Insurance Co. v. Coinstar Inc. was a declaratory judgment action brought by National Union alleging that it had no duty to defend or indemnify the kiosk-based movie rental company Redbox Automated Retail (owned by Coinstar) for a class action suit filed in

[2] Available at http://www.nist.gov/cyberframework/csf_reference_tool.cfm

Illinois. The defendant asserted counterclaims seeking a declaration that National Union was obligated to defend it in two other lawsuits, one in Michigan and one in California.

The Redbox commercial general liability policy provides coverage for "personal injury and advertising injury," which includes "oral or written publication, in any manner, of material that violates a person's right of privacy." The policy excludes losses arising from violations of law.

In February, the court had held that National Union had no obligation to defend Redbox in the Illinois suit since it concerned an alleged violation of the Video Privacy Protection Act and therefore came under the policy's exclusion for violation of law. The current decision involved National Union's obligation in the Michigan and California cases.

In the Michigan case, Redbox is alleged to have violated the Michigan Video Rental Privacy Act by sending its customers' video rental information to third parties. The *National Union* court held that, as with the Illinois case, a violation of the Michigan Act constituted an exclusion under the policy as a violation of law.

The California case concerned an alleged violation by Redbox of the California Song-Beverly Credit Card Act, which prohibits an entity that accepts credit cards from requiring the cardholder to write any personally identifiable information on a credit card transaction form. The plaintiffs argued that Redbox violated this Act by requesting a customer's zip code or email when it conducted a transaction. In analyzing whether Redbox's policy covered the California suit, the court looked first to whether there was any "personal injury or advertising injury." Redbox argued that the California complaint also included allegations as to how Redbox used the information it collected, and therefore included allegations that were not violations of law. However, the court rejected that argument since these additional allegations were not relevant to the single cause of action in the complaint, namely the collection of personal information in violation of the Song-Beverly Credit Card Act. Since the California case was, in effect, a case alleging a violation of law, National Union was not obligated to provide coverage.

The court's holding highlights the risk that companies may face today relying on general commercial policies as protection against privacy and cyberattacks.

Return to Table of Contents

SAFE HARBOR UNDER ATTACK — THIS TIME FROM A US GROUP

In recent months, the EU-U.S. Safe Harbor, which provides a self-certification mechanism for U.S. companies to properly comply with data transfer from the EU to the U.S., has come under increasing attack. Until now, most of these attacks have come from EU regulators and EU-based privacy advocates who have asserted that companies certified to the Safe Harbor do not actually comply with its requirements and that enforcement by the Federal Trade Commission (FTC) has been too lax. A number of EU regulators have called for revisions to the Safe Harbor and, in some cases, its elimination. This argument is now being advanced by at least one U.S.-based advocacy group. On August 14, the Center for Digital Democracy (CDC), a nonprofit privacy advocacy group, filed a Request for Investigation with the FTC, asking the FTC to investigate 30 U.S. companies regarding their Safe Harbor compliance.[3]

The complaint sets forth how these 30 companies are allegedly compiling, using and sharing EU consumers' personal information "without their awareness and meaningful consent," in violation the Safe Harbor framework. The companies include data brokers, data management platforms and mobile marketers. Interestingly, the CDC acknowledged that these companies may not collect "traditional types of personal information." Instead the CDC's focus is that these companies compile identifiers and other information to allegedly create "digital dossiers" of EU consumers.

[3] Available at http://www.centerfordigitaldemocracy.org/sites/default/files/Request%20for%20investigation%20U.S.-EU-SH%202014.08.14.pdf.

According to the CDC filing, these companies: (1) failed to provide accurate and meaningful information to EU consumers in their Safe Harbor declarations and privacy policies; (2) have not been transparent about the nature of their data collection apparatus, "including their networks of data broker partners and even their corporate affiliations;" (3) failed to provide meaningful opt-out mechanisms that EU consumers can find and use to remove themselves fully from "privacy-harming data collection and processing;" (4) claimed to anonymize data despite having sufficient information to identify individuals; and (5) made false claims that they merely act as "data processors" on behalf of others, when in fact their role is much more central to "consumer profiling and targeting." In general, the CDC maintains that these companies all collect, use and share EU consumers' personal information "to create digital profiles about them, analyze their behavior, and use the data to make marketing and related decisions regarding each of them."

The CDC complaint requests that the FTC open inquiries on the 30 companies with respect to three areas of alleged deception:

- misstating their actual purposes and practices of data collection and use, including insufficient disclosures and omitting material information;
- misrepresenting legal facts of importance to EU consumers; and
- merging with and acquiring companies that expanded their data collection and profiling capabilities without adequately updating their Safe Harbor disclosures.

In the CDC's view, the example of these 30 companies demonstrates the "systemic failure" of the Safe Harbor to function as it was intended, and that its needs "to be overhauled." Significantly, the CDC advocates suspending the Safe Harbor until problems are addressed, bringing the its position in line with the more extreme views expressed by certain EU regulators.

Return to Table of Contents

CHALLENGE TO THE SALE OF THE CRUMBS' CUSTOMER LIST

A challenge by the United States Trustee to the sale of Crumbs Bake Shop's customer list in a bankruptcy proceeding serves as a critical reminder of how privacy policies should be drafted.

Those who have been involved with privacy rights for a number of years will recall the challenge that Toysmart.com LLC faced in 2000 when it attempted to sell its customer list through public auction in connection with a bankruptcy proceeding. The FTC moved to enjoin that sale, however, because Toysmart.com had stated in its privacy notice that customers could "rest assured" their information would "never be shared with a third party." In the FTC's view, such a sale would contravene the company's privacy policy and be a deceptive trade practice in violation of Section 5. While Toysmart.com and the FTC eventually entered into a settlement agreement, challenges to the settlement by 47 state attorneys general forced Toysmart.com to eventually destroy the list.

In order to address the Toysmart.com issue, the Bankruptcy Abuse Prevention and Consumer Protection Act (BAPCPA) of 2005 includes a provision that requires the appointment of an independent consumer privacy ombudsman to oversee the sale or lease of the debtor's personal information files unless the debtor's privacy notice explicitly would permit such a sale or lease. The ombudsman is tasked with making a recommendation to the bankruptcy court as to whether the sale should be allowed to proceed. BACPA sets forth a number of factors for the ombudsman to consider including: (1) the debtor's privacy notice, (2) the privacy impact on consumers if the sale proceeds and (3) alternative solutions that might mitigate the privacy impact. Once the ombudsman provides a recommendation, the court must conduct a hearing to assess these factors and non-bankruptcy law.

The issue of selling a customer list in bankruptcy has arisen in connection with the bankruptcy proceedings for Crumbs Bake Shop. The Crumbs privacy policy stated:

> Crumbs Bake Shop is highly sensitive to the privacy interests of consumers and believes that the protection of those interests is one of its most significant responsibilities. In acknowledgement of its obligations, Crumbs Bake Shop has adopted the following Privacy Policy applicable to information about consumers that it acquires in the course of its business. …
>
> Disclosure to Third Parties. We will provide individually-identifiable information about consumers to third parties only if we are compelled to do so by order of a duly-empowered governmental authority, we have the express permission of the consumer, or it is necessary to process transactions or provide our services. …

When Crumbs attempted to sell its customer list in connection with a sale of its assets, the United States Trustee moved for an Order Directing the Appointment of a Consumer Privacy Ombudsman. The U.S. Trustee asserted that the Crumb's privacy policy allows for the transfer of personal information in only three instances: (1) if compelled to do so by a duly empowered governmental authority, (2) if the debtors have the express permission of the consumer, or (3) if it is necessary to process transactions and provide services. As the U.S. Trustee noted, since the sale of the customer lists to a third party does not fall within one of the stated exceptions, the sale of the lists is prohibited. In the words of the U.S. Trustee: "To read the policy differently would render the Debtors' privacy policy meaningless, leading consumers to believe their personal information is protected when in fact, it is not." The U.S. bankruptcy judge agreed and granted the U.S. Trustee's motion.

PRACTICE POINT

The Crumbs issue is an important reminder that any privacy policy should include a statement that personal information may be sold, leased or transferred to a non-affiliated third party in connection with the sale of the business or some or all of the company's assets. This provision is important not only for bankruptcy proceedings, but for M&A activity as well. In this regard, it is important to avoid saying "all or substantially all" of the company's assets in the event the customer list is part of a small class of asset being sold or even the only asset being sold.

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

JESSICA N. COHEN
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

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