Skadden

PRIVACY & CYBERSECURITY UPDATE

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

04.13

INSIDE

LEARN MORE

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

Stuart D. Levi, New York
+1.212.735.2750
stuart.levi@skadden.com

Pierre Servan-Schreiber, Paris
+33.1.55.27.11.30
pierre.servan-schreiber@skadden.com

Shari L. Piré, Paris
+33.1.55.27.11.43
shari.pire@skadden.com

Joshua F. Gruenspecht, Washington, D.C.
+1.202.371.7316
joshua.gruenspecht@skadden.com

Sigrid E. Neilson, New York
+1.212.735.2629
sigrid.neilson@skadden.com

Ken D. Kumayama, Palo Alto
+1.650.470.4553
ken.kumayama@skadden.com

Four Times Square
New York, NY 10036
Telephone: +1.212.735.3000

WWW.SKADDEN.COM

Data-Breach Class Actions After the Supreme Court Decision in *Clapper*

One of the greatest concerns that companies face when they suffer a data breach is the potential for a class action lawsuit by all individuals whose data was effected. Such a case, if successful, could turn a merely troublesome event into one that has significant financial repercussions for the company. However, the Supreme Court's recent decision in *Clapper v. Amnesty International USA*[1] suggests that plaintiffs in such a case might not have standing if they have not suffered any actual harm from the data breach.

In *Clapper*, a group of attorneys and human rights activists challenged the constitutionality of Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA), which allows the attorney general and the director of National Intelligence, acting under the auspices of the Foreign Intelligence Surveillance Court, to authorize surveillance of non-U.S. persons located outside the United States. The plaintiffs alleged that this authority chilled their ability to communicate with certain individuals outside the United States who were essential for them to perform their jobs. The plaintiffs also alleged they were damaged because they sometimes had to pay to travel abroad so they could communicate in person with individuals who might be subject to U.S. government surveillance of their phones and email.

In a 5-4 decision, the Supreme Court held that these plaintiffs did not have Article III Standing to challenge the FISA statute. With respect to the possibility of future harm, the Court held that plaintiffs lack standing unless "injury is certainly impending" since "allegations of possible future injury are not sufficient." The Court noted that here a number of events had to unfold for the plaintiffs to suffer any actual harm, including that the government happened to be targeting for surveillance the same individual with whom plaintiff was then communicating. The Supreme Court's holding thus strikes a serious blow against data breach plaintiffs who argue that although they have not been injured by the data breach, the potential for future harm exists. A defendant in such a case can argue that, as in *Clapper*, such harm is too remote since a series of events would have to unfold for harm to occur: the data would have to fall into the hands of those seeking to do them harm; such individuals would have to attempt to do harm; and, the plaintiff would have to suffer actual loss as a result.

The Court's ruling also strikes a blow against data breach plaintiffs who argue they suffered actual damage because they were "required" to obtain credit monitoring protection or engage in other proactive steps. Such actions can be analogized to the costs incurred by the *Clapper* plaintiffs who spent money to meet their interviewees or clients in-person to avoid the risk of surveillance. The *Clapper* Court rejects such costs as actual damage, noting that they were voluntary and that plaintiffs simply "cannot manufacture standing by incurring costs in anticipation of non-imminent harm."

While class action lawsuits in data breach cases remain a real risk, the *Clapper* decision provides defendants in such actions with an important weapon to argue that there is no standing.

1 No. 11-025 (U.S. Feb. 26, 2013).

California Supreme Court Holds That Song-Beverly Credit Card Act Does Not Apply to On-line Purchases

Introduction

The California Supreme Court recently held that California's Song-Beverly Credit Card Act of 1971 (Song-Beverly Act) — which limits the personal information retailers can collect in a credit card transaction — does not apply to online purchases. The decision, *Apple Inc. v. Sup. Ct. of L.A. County ex rel Krescent*,[2] follows a 2011 decision in which the court said that under the Song-Beverly Act brick-and-mortar retailers could not collect zip code information during credit card purchases. *(See also the discussion of the recent development in Massachusetts regarding the collection of zip codes addressed later in this mailing.)* The court's decision signals that in California, which has been proactive in enacting privacy legislation, the Supreme Court is sensitive to the need of to balance privacy rights with online security requirements.

Background

Section 1747.08 of the Song-Beverly Act prohibits retailers from requesting or requiring any personal information as a condition to accepting credit card payments. "Personal information" is broadly defined as "information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number."[3]

In 2011, the California Supreme Court surprised many observers with its decision in *Pineda v. Williams-Sonoma Stores, Inc.*, in which the court held that ZIP codes constitute personal identification information, such that a retailer collecting ZIP codes along with credit cards violates the Song-Beverly Act.[4] According to the *Pineda* court, the legislative history of the relevant provisions of the Song-Beverly Act indicate that the California Legislature was concerned about retailers obtaining consumers' "additional personal information for their own business purposes — for example, to build mailing and telephone lists which they can subsequently use for their own in-house marketing efforts, or sell to direct-mail or tele-marketing specialists, or to others."[5]

In *Apple*, plaintiff David Krescent filed a complaint alleging that Apple Inc. (Apple) violated the Song-Beverly Act by requiring that he provide his home address and telephone number as a condition to purchasing downloadable products from Apple. Krescent sought statutory penalties for the alleged violations and certification of a class comprising individuals who were similarly harmed.

Apple filed for a demurrer, essentially requesting that the case be dismissed for failure to state a claim. After losing at the lower court levels, Apple appealed to the California Supreme Court.

Competing Policies: Privacy vs. Preventing Credit Card Fraud

In support of the demurrer, Apple asserted that online retailers have legitimate business reasons for collecting personal information, chief among them to combat fraud. Apple also contended that the Legislature could not have considered the balance between consumers' right to privacy and the online retailers' desire to prevent fraud because the Internet, as we know it, did not exist in 1990. The Legislature had no way of conceiving of the nature of online transactions. Implicit in Apple's argument is the notion that online sales are different enough from the sales methods that existed in 1990 that a different balancing of the policies at issue is required.

The majority found that in enacting Section 1747.08(d), the California Legislature was concerned about fraud on consumers and retailers alike. For example, that section permits retailers to request photo identification before accepting a credit card payment. Similarly, that section permits a retailer to "record the customer's driver's license number or similar information when the customer does not make the credit card available for verification, presumably so that the customer may be

---

2 Available online at www.courts.ca.gov/opinions/documents/S199384.pdf.

3 Cal. Civ. Code § 1747.08(b).

4 51 Cal. 4th 524 (2011).

5 *Id.* at 534-35 (quoting Sen. Com. on Judiciary, Analysis of Assem. Bill No. 2920 (1989-1990 Reg. Sess.) as amended June 27, 1990, pp. 3-4) (internal quotes omitted).

identified and located in the event of a problem with the use of the credit card." Thus, the majority reasoned, the Legislature did not intend to protect consumer privacy "at the cost of creating an undue risk of credit card fraud." In siding with Apple, the court determined that the courts are not the correct forum to decide how best to balance the need to combat fraud against consumers' right to privacy.

The majority also noted that online transactions have a greater risk of credit card fraud than sales at brick-and-mortar retailers because "an online retailer cannot visually inspect the credit card, the signature on the back of the card, or the customer's photo identification."

Krescent argued that, in 2011, the Legislature amended the Song-Beverly Act to allow gas stations to collect zip code information "solely for the prevention of fraud, theft, or identity theft."[6] According to Krescent, this 2011 amendment confirmed that all retailers, including retailers conducting business remotely, are governed by the statute — as there would be no need for an amendment if remote transactions were not covered. The majority disagreed, noting that "[c]ompared to ordinary brick-and-mortar retailers, gas stations with payment island automated cashiers may indeed have heightened fraud concerns, and it would make sense for the Legislature to grant them more leeway to record personal identifying information."

Practice Notes

The court's decision appears to have been driven by the belief that the relevant provisions of the Song-Beverly Card Act are out of date for e-commerce sales and the risk of identity theft. Specifically, the Legislature intended for retailers to be able to combat fraud, but the statute, as currently drafted, does not provide a mechanism for online retailers to do so. The court invited the Legislature to update the act if it determined that online purchases also should be covered. As might have been expected, the Legislature is in the process of doing just that.[7] As of the date of this publication, the bill has been referred to the Senate Committee on Judiciary, where a hearing on the bill will likely take place later this month.

The decision also highlights that the California Supreme Court is carefully analyzing the applicability of traditional privacy laws to the online world, and acknowledges that the calculus in balancing privacy and security may be different depending on the type of transaction in which the consumer has engaged.

Massachusetts Privacy Law Prohibits Collection of ZIP Codes in Retail Purchases

A recent decision in Massachusetts highlights the reality that zip codes are quickly becoming the new frontier in the tension between privacy rights and marketing activities. In *Tyler v. Michaels Stores, Inc.*,[8] the state's highest court ruled that ZIP codes are a type of personal information that cannot be collected in conjunction with credit card purchases. This case follows a similar ruling in 2011 by the California Supreme Court, which held that, under California's Song-Beverly Credit Card Act,[9] retailers could not collect zip code information.[10] The concern is that retailers link the zip code with the name on the card to build a record of individuals and their purchase history. Retailers argue that they collect ZIP codes and other generic consumer information in order to better serve consumers. For example, collecting ZIP codes from customers may help retailers in deciding where to open new store locations. Nonetheless, the California case led to an onslaught of privacy litigation in that state.

---

6 Cal. Civ. Code § 1747.08(c)(3)(B).

7 See Cal. Senate Bill No. 383 (Feb. 20, 2013).

8 No. SJC-11145, 2013 WL 854097 (Mass. Mar. 11, 2013).

9 Cal. Civ. Code §§ 1747, et seq.

10 *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524 (2011).

In *Tyler,* the lead plaintiff disclosed her ZIP code at Michaels craft store under the mistaken impression that it was required to complete her credit card purchase. However, the card issuer did not require the retailer to request this information. The store instead used the ZIP code to obtain the customer's home address and telephone number from publicly available databases and sent unsolicited marketing information.

The court found that the recording of ZIP codes constituted a collection of "personal identification information" in connection with a credit card transaction and was thus an unfair or deceptive trade practice under state commercial privacy law.[11] The statute explicitly includes as "personal identification information" a consumer's address and telephone number. The court held that since a consumer's ZIP code can be used to find a consumer's address and telephone number through publicly-available databases, it also could be considered personal identification information protected under the law.

In its decision, the Massachusetts high court reversed a lower court decision that had interpreted the Massachusetts law as being aimed at preventing identity fraud. Since Michaels craft store was not engaged in such activity, the lower court held that there was no recognizable harm to the plaintiff. The Massachusetts Supreme Judicial Court viewed the statute in much broader terms, finding that it was passed in response to concerns over the "disclosure of personal information leading to the identification of a particular consumer generally" and that a finding of identity fraud is not a prerequisite for recovery under the law. However, the court also held that the law requires plaintiffs to show actual injury caused by the act or practice claimed to be unfair or deceptive, which may include: (i) actual receipt of unwanted marketing materials or (ii) the merchant's sale of personal identification information to a third party. This is a notable divergence from the earlier California decision, which found that an invasion of privacy occurred from the collection of a ZIP code alone, without further injury.

It remains to be seen how much evidence Massachusetts plaintiffs will need to provide in order to show that the collection of their ZIP codes led to a downstream privacy invasion, but the injury requirements will make it more difficult to bring a case under *Tyler* than under the California law and may lead to less follow-on litigation than in California.

Some commentators have noted that rulings of this type seem antiquated in light of current online marketing practices where internet retailers are able to request and gather tremendous amounts of information about consumers through cookies, social media integration and other methods. But perhaps cases like this serve as a signal that the increase in the amount of personal information consumers are willing to share online correlates to a decrease in their tolerance for mailed communication and dissemination of their home addresses. These decisions also may indicate courts' general willingness to protect against consumer privacy invasions, which could have future consequences for Internet retailers as well.

Recent FTC Settlement Highlights Agency's Views on 'Privacy by Design'

The Federal Trade Commission (FTC) recently entered into a settlement agreement with one of the leading mobile device manufacturers, HTC America, Inc. (HTC), arising from security vulnerabilities found in HTC's customization of mobile software applications.[12] The proposed settlement marks the first time the FTC has brought and settled claims of unfair practices in the context of software security.[13] As such, it presents another example of the FTC's increased vigilance in the mobile privacy

11 Mass. Gen Laws ch. 93, § 105(a).

12 See Agreement Containing Consent Order, *In the Matter of HTC America Inc.*, No. 122-3049 (Fed. Trade Comm'n Feb. 22, 2013), available at http://www.ftc.gov/os/caselist/1223049/130222htcorder.pdf.

13 As further described below, the proposed consent order was published by the FTC for public comment and, accordingly, is not yet final.

arena and its willingness to use Section 5 of the FTC Act to enforce certain privacy practices even when no privacy-specific legislation yet exists.

Background

HTC manufactures and sells mobile devices based on both the Android and Windows Mobile operating systems. In order to distinguish its products from those of competitors, HTC customizes the mobile devices and its software by adding or modifying various pre-installed applications and components. However, according to the FTC, during the design and customization process, HTC failed to use reasonable and appropriate security measures and, consequently, introduced security vulnerabilities to the devices that could enable third parties to access sensitive customer information.[14] Namely, the FTC noted HTC failed to:

- Implement an adequate program to assess the security of its products;
- Implement adequate privacy and security guidance or training for its engineers;
- Conduct assessments, audits, reviews or tests to identify potential security vulnerabilities;
- Follow well-known and commonly accepted secure programming practices, including those described in the operating system's guides for manufacturers and developers; and
- Implement a process for receiving and addressing security vulnerability reports from third parties.

By way of example, the Android operating system utilizes a security model requiring that third-party applications be granted user "permission" before accessing certain sensitive device functionality or information. To that end, "permission check" code is typically included in device software to verify that a third-party application has the requisite permissions when it requests access to such functionality or information. However, HTC pre-installed a customer application on its Android-based devices that allowed users to download and install applications outside the normal Android installation process and that did not include any "permissions check" code. As a result, other third-party applications could instruct this customized application to download and install additional applications to the device without the user's knowledge or consent. Users were not given an option to uninstall or remove this HTC application. According to the FTC, this vulnerability was present on upwards of 18 million mobile devices and placed consumers at risk of financial and physical injury and other harm.

In addition to the various allegations regarding HTC's failure to employ reasonable and appropriate security practices, the FTC also asserted that certain statements made to device users were false or misleading representations. For example, HTC's user manual for its Android devices implied that downloaded applications would require the user's consent in order to access their personal information or certain functions on the device. However, as noted above, the security vulnerabilities introduced in software could bypass the need for user consent.

Proposed Consent Order

Under the terms of the proposed consent order, HTC must establish, implement and maintain a comprehensive written security program that is reasonably designed to (i) address security risks related to developing and managing its mobile devices[15] and (ii) protect the security, confidentiality and integrity of "covered information," *i.e.*, personally identifiable information collected through, stored on, captured with or transmitted through HTC's mobile devices.

---

14 *See* Complaint, *In the Matter of HTC America Inc.*, No. 122-3049 (Fed. Trade Comm'n Feb. 22, 2013), available at http://www.ftc.gov/os/caselist/1223049/130222htccmpt.pdf.

15 The FTC made clear that the obligations under the security program extended only to HTC's integration, modification or customization of third-party software on its mobile devices and did not generally make HTC responsible for otherwise identifying and correcting any vulnerability in noncustomized third-party software.

This security program, which must be coordinated by an HTC employee who is accountable for it, must, in part:

- Identify material internal and external risks to the security of HTC mobile devices that could result in unauthorized access to or use of certain device functionality;
- Identify material internal and external risks to the security, confidentiality and integrity of covered information that could result in unauthorized use or disclosure of such information;
- Include assessments of the safeguards put in place to control the foregoing risks that covers each area of relevant operation, including:
  - Employee training and management;
  - Product design, development and research;
  - Software design and testing, including secure engineering and defensive programming; and
  - Review, assessment and response to third-party security vulnerability reports.
- Develop reasonable steps to select service providers capable of maintaining security practices consistent with the consent order, and require such service providers by contract to implement and maintain appropriate safeguards; and
- Modify the security program in light of the results of testing the program, any material changes to HTC's operations or business, or other circumstances HTC knows or should know may materially impact the security program's effectiveness.

The proposed consent order also prohibits HTC from misrepresenting, expressly or by implication, the extent to which HTC, or its mobile devices and related services, protect the security of device functionality or the security, confidentiality or integrity of covered information. HTC also must develop and release security patches to fix the vulnerabilities identified by the FTC. Finally, HTC must obtain initial and biennial third-party security assessments for a period of 20 years and satisfy certain similar compliance obligations.

Although HTC agreed to the terms of the consent order and the FTC voted to accept it, the FTC did elect to provide the public with an opportunity to comment on the consent order before it is finalized. A description of the proposed Consent Order was published in the Federal Register for a 30-day public comment period, which ended on March 22, 2013. The FTC currently is reviewing comments it received and is expected to announce whether the consent order is final in the near future.

Practice Points

The FTC's enforcement action against HTC is consistent with the FTC's declared agenda of promoting a privacy framework based in part on "privacy by design." As noted in a 2012 FTC final report on consumer privacy, "privacy by design" embodies the principle that companies should "promote consumer privacy throughout their organizations and at every stage of the development of their products and services," including by implementing and maintaining substantive protections and procedures regarding data security, reasonable collection limits, sound retention practices and data accuracy.[16] Essentially, the FTC believes companies need to think through and address data security and privacy issues proactively at all stages, including development, not reactively once something has gone awry.

The HTC settlement serves as an important reminder that while "privacy by design" is not a statutory or regulatory requirement, it should be seen as a necessary best practice in light of recent FTC enforcement activity. The HTC settlement also provides insight in terms of those data security practices the FTC views as essential to satisfy a "privacy by design" approach. ***As part of its continued efforts to ensure that companies factor in security risks when developing mobile devices and applications, the FTC also will host a public forum on malware and other mobile security threats on June 4, 2013.*** "Privacy by design" also should be viewed as a critical risk-mitigation technique. Thinking

16 *See* Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (2012) at 22-34, available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.

through security risks, and the ways in which those risks can be minimized at the outset of the design process, will help prevent those risks from coming to fruition. Moreover, companies now operate in an age of increasing public and media backlash for engaging in practices that may not meet consumer privacy or security expectations. Fostering a proactive approach towards consumer privacy and security will help companies navigate issues that may arise.

Finally, the FTC's claims against HTC are even more interesting when considered in light of the pending litigation between the FTC and the Wyndham hotel chain. The FTC alleged that Wyndham, which suffered a series of privacy breaches caused by hackers, failed to maintain reasonable and appropriate security procedures and therefore committed an unfair act or practice in violation of Section 5. Wyndham has moved to dismiss all charges brought by the FTC, arguing that the FTC's attempts to mandate a company's data security practices far exceeds the agency's authority to regulate unfair acts or practices and circumvents the efforts of Congress and the White House to determine how best to address privacy and cybersecurity issues.[17] The FTC's claim that HTC failed to follow a "privacy by design" approach even though there is no formal requirement to do so arguably provides another example of the concerns expressed by Wyndham.

17 See Motion to Dismiss, *Fed. Trade Comm'n v. Wyndham Worldwide Corporation, et al.*, No. CV 12-1365-PHX-PGR (D. Ariz. Aug. 27, 2012).

Flaming Worms, Stuxnets and Other Cyber Threats — The European Union's Response

The media is replete with reports of a botnet onslaught paralyzing Spamhaus, flaming worms usurping strategic information in the Middle East and a stuxnet super weapon wreaking physical damage to Iran's nuclear reactors. Behind these barbaric neologisms hides a real and serious threat to most corporations: cyberattacks. Given the importance and breadth of electronic data stored within corporations today, any unauthorized access could lead to serious consequences ranging from a public relations nightmare to actual, significant monetary damages. When it comes to cyber-attacks, recent examples demonstrate that no organization is too big or too sophisticated to be immune.

In light of the risks involved, corporations must take appropriate measures, while considering the ever-evolving global regulatory regime. In addition to U.S. efforts to address cybersecurity risks,[1] the European Commission published a proposed directive on network and information security.[2] If and when it passes, the directive shall trigger significant changes in the way European companies and those doing business in Europe use information technology.

Propagation and Costs of Cyber-Attacks

Increases in the number of hackers and in illegal infiltration into public and private information systems have caused governmental authorities and the private sector to focus on the exposure of critical information systems to cyber-attacks. As has been widely reported, the variety of cyber criminals include teenage hackers, opportunists attempting to steal money, "sophisticated" hackers who appear motivated by the desire to cripple corporate systems and state actors using cyber weapons as a means of extending real-world warfare and espionage into the digital realm. Economic cyber espionage is particularly pervasive. The French finance ministry was infiltrated at the end of 2010 and in 2012, and even the offices of former President Sarkozy were infected.[3]

As of 2012, only one out of every four companies in the European Union (EU) had an established and regularly reviewed information and communications technology security policy, leaving many Member States vulnerable and ill-prepared to stave off the growing number of sophisticated cyber-attacks.[4] Recognizing the risks facing its constituents, the Commission now seeks to implement new regulatory measures in an effort to enhance cybersecurity. The French and German governments are among those Member States echoing the need for decisive action.[5]

Cybersecurity Measures Taken in the EU

On February 7, 2013, the European Commission published a proposed directive on network and information security designed to further the Commission's cyber-defense strategy which calls for an open, safe and secure Internet. To meet these goals, the Commission stressed that all 27 Member States must work as a unit with common legislative objectives and requirements, concluding that the voluntary approach to network and information security employed to date is insufficient to provide the desired results.[6] The Commission noted that Member States are currently not operating on a level playing field — some Members have both greater capabilities and are better equipped to defend their network information systems than others.[7] This disparity in capabilities and preparedness is viewed by the Commission as an impediment to creating effective collaboration and cooperation among the Member States, without which EU-wide cyber-resilience may remain illusory.[8]

Under the current regulatory framework, only telecommunications companies are required to implement risk management strategies and report network information systems incidents,[9] while only data controllers[10] are required to implement security mechanisms to ensure the protection of personal information.[11] As such, current legislation leaves a void for addressing incidents in sectors other than telecommunications, such as transportation, stock exchanges, aeronautics, cryptology, media, energy and banking, all of which can be adversely affected by information and infrastructure breaches.[12] Absent a more comprehensive legal regime, the Commission determined that Member States may lack effective incentives to report or evaluate breaches, manage risks or design effective cyber-solutions.[13]

The Proposed Directive is aimed at, among other things, bridging this gap. Should it be adopted, the Proposed Directive will require public administrations and market operators to implement and maintain risk management strategies and to report significant network information security breaches to the applicable competent authorities.[14] The Commission will be vested with the authority to dictate the requisite formats and procedures for notification of such incidents.[15] In addition, public administrations and applicable market operators will be required to furnish information necessary to assess the security of their network and information systems and be subject to regular security audits, the results of which would be made available to the competent authorities.[16] Failure to meet security assessments could result in sanctions.[17]

What Companies Would Be Affected?

The Proposed Directive defines a market operator as including certain information society services providers and the operators of critical infrastructure "essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health."[18] An annex to the Proposed Directive provides a non-exhaustive list of market operators, which list includes social networks, search engines, cloud computing services, electricity and gas operators, businesses operating refineries or other treatment facilities, air carriers, railways and businesses in the logistics services sector, certain credit institutions, central counterparty clearing houses as well as hospitals and health care facilities.[19]

Differences in EU and U.S. Proposed Cybersecurity Regulation

The Proposed Directive is being debated in Europe at the same time as a nominally less prescriptive regulatory regime is taking shape in the United States. A recent U.S. executive order (the Cybersecurity Order) focuses on information sharing and regulation related to critical infrastructure cybersecurity. Such "critical infrastructure" includes those private sector assets whose loss, disability or destruction would adversely affect U.S. security, public health or economic prosperity.[20] The Presidential Directive accompanying the Cybersecurity Order makes clear that the same classes of market operators that would be covered by the Proposed Directive in the EU may ultimately face additional regulation in the U.S. under the Cybersecurity Order. The classes of entities covered in the proposed regulations are not, however, completely parallel. By contrast to the Proposed Directive, the Cybesecurity Order and Presidential Directive explicitly identify food and agriculture and critical manufacturing among the covered sectors, but carves out cloud computing applications, social media and search engines.[21]

The Cybersecurity Order establishes a process under which the Department of Homeland Security (DHS) would assess the need for regulation of cybersecurity measures taken at critical infrastructure businesses,[22] and tasks the National Institute of Standards and Technology (NIST) with developing a framework designed to provide critical infrastructure owners and operators with proposed measures and controls which, if implemented, may reduce cyber-risks.[23] While the Cybersecurity Order states that private sector implementation of the framework is voluntary, certain sector-specific regulatory agencies have been asked to address deficiencies found by DHS.[24] More specifically, the Cybersecurity Order requires each such agency to review the extent of its regulatory authority, together with the DHS findings. If regulations are found deficient to address cybersecurity risks, the agencies would be directed to take actions within each such agency's power to enforce compliance by such businesses with the recommendations provided in the NIST framework.[25] Accordingly, critical infrastructure businesses operating in the U.S. may deem it prudent to treat the NIST framework much like their counterparts operating in the EU may treat the Proposed Directive — as a compulsory regulatory regime.

As a result of the different approaches to regulating private sector networks and systems taken in the U.S. and EU, operators should not assume that security measures instituted to satisfy one regulatory or legislative regime will suffice under another. Those operators who may be subject to either regime should pay careful attention as both approaches continue to take shape over the next several months.

Next Steps

The Proposed Directive was submitted to the European Parliament and the European Council for review and adoption. If adopted, the Member States will have 18 months following adoption of the Proposed Directive to transpose or implement it into their respective national laws. In the interim, operators falling within the scope of the Proposed Directive should begin to assess the security of their current systems as if the Proposed Directive were adopted so that they can begin to see where they may have vulnerabilities to be addressed.

More generally, all private sector companies should continue to monitor this area closely and take appropriate steps to minimize the risks associated with cybersecurity threats.

End Notes for the "Flaming Worms, Stuxnets and Other Cyber Threats — The European Union's Response" article appear on the following pages.

END NOTES – "Flaming Worms, Stuxnets and Other Cyber Threats — The European Union's Response"

1 *See* Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, "Privacy and Cybersecurity Updated: President Issues Cybersecurity Executive Order," P*rivacy & Cybersecurity Update*, Feb. 13, 2013 at http://www.skadden.com/newsletters/Privacy_and_Cybersecurity_President_Issues_Cybersecurity_Executive_Order.pdf; see also Antoinette C. Bush, Stuart D. Levi, Ivan A. Schlager, John M. Beahn and Joshua F. Gruenspecht, "Privacy & Cybersecurity Update: NIST Issues Request for Information on Critical Infrastructure Cybersecurity Practices," Mar. 5, 2013 at http://www.skadden.com/sites/default/files/publications/Privacy_Cybersecurity_Update_%20NIST_Issues_Request_for_Information_on_Critical_Infrastructure_Cybersecurity_Practices.pdf.

2 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, Brussels (Proposed Directive), Feb. 7, 2013 at http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf.

3 Saskya Vandoorne, "Cyber attack hit French Finance Ministry," government says, CNN, Mar. 7, 2011 at http://www.cnn.com/2011/WORLD/europe/03/07/france.cyberattack/index.html?_s=PM:WORLD; Emmanuelle Paquette, "Cyberattaque contre l'Élysée: la défense de Washington," *L'Express*, Nov. 20, 2012 at http://lexpansion.lexpress.fr/high-tech/cyberattaque-contre-l-elysee-la-defense-de-washington_361245.html.

4 *See* Neelie Kroes' European Commission speech, "Towards a coherent international cyberspace policy for the EU," Jan. 30, 2013, delivered in connection with the Global Cyber Security Conference in Brussels, at http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=9568 (Commission Speech), p. 3; see also European Commission press release "EU Cybersecurity plan to protect open internet and online freedom and opportunity," Feb. 7, 2013 at http://europa.eu/rapid/press-release_IP-13-94_en.htm (EU Press Release).

5 The French government recommends strengthening security standards imposed on businesses operating in critical sectors, developing risk-management tools and making them available to small and mid-sized businesses and running, within the confines of the legal framework, tests on software security and the means of responding to attacks. Antton Achiary, Joël Hamelin and Dominique Auverlot, *La Note d'analyse, nº324, Centre d'analyse stratégique*, March 2013. The German Federal Ministry of the Interior published proposed amendments, which if adopted, would require critical infrastructure operators to disclose cybersecurity breaches to the German Federal office for Information Security. *See* First draft of the Federal Ministry of the Interior at http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf;jsessionid=B3769DFABA3DFAD5C7FE3DF0B59948F9.2_cid287?__blob=publicationFile.

6 Explanatory Memorandum to the Proposed Directive § 1.1 (Directive Memo).

7 Id.

8 Id.

9 See Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, Art. 13a, amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services. French regulations are broader. In France, telecommunications operators and internet service providers are required to report data security breaches to French authorities (*Commission nationale de l'informatique et des libertés*). See Ordonnace nº2011-2012 du 24 *août 2011 relative aux communications électroniques*.

10 Data controllers are "any natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data". Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the "Data Protection Directive"). Banks, airlines, railways, hospitals and hotels provide a few examples of data controllers. On January 25, 2012, the Commission published a proposed regulation designed to replace the Data Protection Directive. *See* Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on free movement of such data at http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf.

11 See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

12 *See* Directive Memo.

13 *See* Cybersecurity Strategy of the European Union: *An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the

Committee of the Regions, Feb. 7, 2013, p. 6 at http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.

14 Proposed Directive Art. 14. Microenterprises are exempt from risk-management and notification requirements under the Proposed Directive. *See Id.*, which defines microenterprises within the meaning established in Art. 3 of Commission Recommendation 2003/361/EC, May 6, 2003 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF.

15 *Id.*

16 *Id.*

17 See Proposed Directive Art. 17, which provides that Member States shall adopt rules on sanctions applicable to infringement of national provisions adopted pursuant to the Proposed Directive.

18 Proposed Directive Art. 3.

19 Proposed Directive Annex II.

20 The White House – Office of the Press Secretary, "Executive Order: Improving Critical Infrastructure Cybersecurity," Feb. 12, 2013, §2. The presidential directive accompanying the Cybersecurity Order defines critical infrastructure as including the following 16 sectors: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear services, transportation systems and water and waste water systems. *See Presidential Policy Directive PPD-21: Critical Infrastructure Security and Resilience*, Feb. 12, 2013 (Presidential Directive).

21 "The Secretary [of Homeland Security] shall not identify any commercial information technology products or consumer information technology services under this section." Cybersecurity Order § 9.

22 Cybersecurity Order §10.

23 Cybersecurity Order § 7a.

24 Cybersecurity Order §10.