EYE ON PRIVACY

MAY 2012

Welcome to the inaugural issue of *Eye on Privacy.*

Privacy and data security may very well be among the most pressing issues facing companies today, especially given the dynamic regulatory landscape. In just the past few months, the White House and the Federal Trade Commission each released a report outlining a new framework to govern privacy and data security in the United States; the FTC and state attorneys general continued their steady drumbeat of law enforcement; a national cybersecurity bill was introduced in Congress; and the European Union proposed a new data-security regulation that would impose substantial fines on companies that experience data intrusions. And, of course, private class action litigation continues.

Staying current on these crucial issues can be daunting, whether you work on them every day or only on occasion. By launching this newsletter, we hope to help you understand and navigate the privacy landscape.

Please let us know how we're doing by contacting us at **PrivacyAlerts@wsgr.com**. We welcome your feedback and questions, and your thoughts on any topic that you'd like us to address.

Lydia Parnes
Partner, Wilson Sonsini Goodrich & Rosati

Ninth Circuit Holds That Computer Fraud and Abuse Act Does Not Apply to Use of Information Obtained through Authorized Access

By Michael Rubin

In an opinion with significant implications for trade secrets, employee mobility, privacy, and Internet users broadly, the Ninth Circuit Court of Appeals on April 10, 2012, issued its decision in *United States v. Nosal*. Writing for the *en banc* court, Chief Judge Alex Kozinski addressed the proper scope of the federal Computer Fraud and Abuse Act's (CFAA's) prohibition against using a computer in a way that "exceeds authorized access." Building on its prior case law, the court held that while the CFAA forbids unauthorized access to information, it does not prohibit the misuse of information initially obtained through authorized access.

In *Nosal*, the defendant, David Nosal, a former employee of the Korn/Ferry International Corporation, directed current Korn/Ferry employees to use their authorized access to a company database in order to download confidential information and pass it on to him. Those acts were a violation of the company's written policy. The Ninth Circuit rejected the prosecution's argument that authorized access to a computer system for an unauthorized purpose violates the CFAA. The court expressed concern that such a reading would criminalize millions of Americans' day-to-day computer activities.

This decision limits the use of the CFAA in the Ninth Circuit as a vehicle for trade secret misappropriation claims. While employers have made increasing use of the statute in recent years in actions against former or departing employees, *Nosal* shuts the door on that practice by clarifying that the violation of a corporate computer use policy is not grounds for CFAA liability. So long as an employee is permitted to access a device that contains information, the CFAA does not cover later misuse of the information obtained on that device. The court's decision leaves open other avenues of recourse for employers, such as state contract and trade secrets laws.

By holding the CFAA inapplicable to situations where computer access is authorized, *Nosal* also should constrain the act's application in consumer protection actions based on the behavior of software voluntarily installed by a user. Additionally, the CFAA no longer may serve as a basis for claims premised on violations of terms of service agreements or other computer use contracts, leaving those types of claims to be litigated through other causes of action. However, since the Ninth Circuit's interpretation of the CFAA is in direct conflict with the position taken by several other federal courts of appeals, *Nosal* may help lay the groundwork for review of this issue by the U.S. Supreme Court.

Lydia Parnes

Gerry Stegmaier

Privacy, New Media, and Data: Lessons for Business Leaders and Their Advisors

By Lydia Parnes and Gerry Stegmaier

"Most of the online world is based on a simple, if unarticulated, agreement: consumers browse Web sites free, and in return, they give up data—like their gender or income level—which the sites use to aim their advertisements. The new head of the Bureau of Consumer Protection at the Federal Trade Commission, David C. Vladeck, says it is time for that to change."
— *The New York Times*, August 4, 2009

"American consumers can't wait any longer for clear rules of the road that ensure their personal information is safe online. As the Internet evolves, consumer trust is essential for the continued growth of the digital economy. That's why an online privacy Bill of Rights is so important. For businesses to succeed online, consumers must feel secure. By following this blueprint, companies, consumer advocates, and policymakers can help protect consumers and ensure the Internet remains a platform for innovation and economic growth."
— President Obama, February 23, 2012, while releasing the "Consumer Privacy Bill of Rights"

Changing Circumstances Put a Premium on Marketplace and Regulatory Intelligence

Assessing and overcoming risk is the bread and butter of every entrepreneur and investor. Indeed, your very survival requires that you identify risks and execute better than your competition. Online media and data companies—such as analytics businesses, social networking sites, advertisers, and ad networks—increasingly are finding that privacy and data protection issues can make or break their businesses. Proposals by the federal government to Congress and in regulatory rulemaking, questions about the commercial practices of many Internet business models, and the prospect of new, comprehensive privacy legislation all pose a potential risk for many online businesses. In this context, understanding privacy and data protection issues and their significance to consumers—and regulators—is a matter of vital importance.

Privacy Risks Are Significant

Privacy and data protection long have been critical issues for entrepreneurs in new media and online ventures. For example:

- Xanga, a provider of blogging and other user-generated-content features, paid a $1 million civil penalty in connection with allegations that the company violated the Children's Online Privacy Protection Act. The site allegedly represented that it did not collect personal information from children under 13 years of age, yet the company was found by the Federal Trade Commission to have knowledge that some young children had registered for and provided personal information to

the service. In addition to the fine, considerable negative press attention, and business distraction garnered by the incident, the company was required to significantly improve its ongoing compliance measures.

- Facebook encountered allegations that its Beacon program, which enabled the sharing of information between the well-known social networking site and e-commerce sites such as video rental, video game, jewelry, and retail businesses, violated consumer privacy. Although Facebook's CEO publicly apologized and the company quickly stopped automatically sharing information as part of its terms of service, a consumer class action still was filed. Class action litigation followed, with a settlement of $9.5 million being paid to create a new privacy foundation "to fund projects and initiatives that promote the cause of online privacy, safety, and security."

- The chief technology officer of AOL resigned after the company allegedly released 20 million keyword searches for more than 650,000 users. Although the data was made accessible solely to researchers, it was later revealed that the information could be, and was, used to identify individual users. A class action lawsuit was filed seeking at least $5,000 for each affected individual. Consumer and regulator concerns over the use and retention of search data continue to be a flashpoint.

- Sometimes a particular type or method of information collection can touch off a firestorm of controversy. Regulatory and privacy concerns over the collection, use, and disclosure of Internet browsing data by Internet service providers (ISPs) to serve advertising aims captured the attention of popular-media and privacy advocates. The CEO of Nebuad, an ISP-based online behavioral advertising company, resigned following Congressional hearings on the company's business practices. Soon thereafter, the business shut down and similar competitors faced difficulty funding operations. Expensive class action litigation followed and Nebuad and a number of its ISP customers were named as defendants.

Each of these examples demonstrates the ongoing importance of understanding privacy and consumer protection concerns arising out of the collection, use, and disclosure of information online. Regardless of the outcome of a case or investigation, the professional and attorneys' fees associated with investigating and defending these matters easily can exceed $1 million. The costs to the business in terms of reputation and momentum can be many times that amount, and may come at critical times in the life of the enterprise. From these and similar experiences, important lessons for entrepreneurs engaged in social media, user-generated content, analytics, and online advertising emerge.

Lessons for Business Leaders

Consumer and regulator perceptions can be as important as the law. Earning consumer trust remains critical where data collection is an important aspect of the business. Established companies have demonstrated that a business can collect enormous amounts of information about what their customers read and buy, where they travel, and more, all while maintaining their trust. Transparency is an essential component of establishing this trust relationship: by providing simple and understandable information about those practices and building a reputation and brand synonymous with fair information practices, any company can bolster its credibility and ultimately its ability to withstand scrutiny of its privacy practices.

Incorporating privacy and data protection into product planning is essential. Increasingly, privacy is becoming a product feature and competitors are seeking to differentiate themselves with their privacy practices. The ability to differentiate a product based on privacy and protection of data can be especially important to businesses dependent upon the continued growth of social media. The Federal Trade Commission encourages "privacy by design."

Changes in market conditions and perceptions regarding privacy and data protection can have devastating effects. Some consumers are demanding greater control and transparency over data generated by their activities, and advocates for greater privacy and user control have become increasingly vocal. Regulators in the European Union and advocates in the United States have pressed industry to delete data that businesses maintain is critical to product development. Collecting and maintaining anonymous data or even data that can be linked to individuals only with considerable effort has been criticized. The long-standing belief that businesses own the information they obtain about their customers continues to be challenged by an emerging marketplace reality that consumers often expect the right to control such data gathering. The importance of these issues has caused businesses to very quickly and publicly change course, and even seems to have resulted in the wholesale rejection of certain business models.

The importance of privacy and data protection is easily underestimated. Research by the Ponemon Institute suggests that CEOs recognize that privacy and data protection efforts contribute to the success of their brands and are good investments. At the same time, the research also suggests that CEOs, when compared with other C-level executives, are more likely to underestimate security risks related to data held by their companies. Although the importance of privacy and security to brands is widely recognized, implementing meaningful controls and demonstrating adequate return on investment for such controls to upper management continue to be a challenge.

Legal Obligations Continue to Increase

Privacy and data protection issues converge at the intersection of marketing, law, and revenue. Free or nearly free services require a value exchange for the underlying businesses. The ability to monetize data, through advertising or otherwise, remains a fundamental part of the exchange. Legal issues become ever more complex and important in this marketplace, as companies, officers,

and directors are increasingly held accountable for the collection, use, disclosure, and, ultimately, stewardship of data.

FTC and State Law. Numerous laws create obligations to ensure that businesses do not unfairly or deceptively collect, use, or disclose data. The Federal Trade Commission uses its authority to regulate unfair and deceptive trade practices to police these issues and has created a division directed specifically at privacy. As a result, the FTC has brought over three dozen cases challenging the privacy and information security practices of companies large and small. Many states have similar laws, and state attorneys general have actively and publicly sought to hold businesses accountable for their information practices.

Identity Theft and Security Requirements. Beyond privacy, increasing risks and concerns about identity theft have led to numerous requirements that businesses take reasonable steps to secure data that they collect, use, or disclose. Virtually every U.S. state now has a law requiring that consumers be notified in the event of a security breach, and this trend has spread outside of the U.S. as well.

Industry-Specific Legal Requirements. Specialized statutes often create regulatory obligations that are complicated and difficult for emerging enterprises to implement. Privacy and data protection laws regulate health, finance, telecommunications, cable, and movie rental businesses, as well as many other segments of the economy. Businesses that seek to sell into these verticals often find themselves faced with contractual obligations or terms directed at ensuring that these regulatory requirements are met—and quite often even exceeded. Moreover, agreeing to indemnify for failure to meet these obligations, or even agreeing by contract to meet them, often is no longer enough for these customers. Large enterprises increasingly conduct thorough due diligence and use audits to ensure compliance from their vendors and suppliers.

Criminal and Individual Liability. Finally, getting things wrong can lead not only to problems for businesses, but also for officers and directors. Shareholders and others increasingly have sought to hold officers and directors personally responsible for privacy and data protection matters, including as fiduciaries to their organizations. At least since the *Caremark* case in the Delaware Chancery Court in 1996, commentators have suggested that the duties of officers and directors likely extend to the protection of intangible

assets, including data and personal information. Because of the public attention associated with many high-profile security breaches, these issues increasingly are discussed in the boardroom. Moreover, particularly in Europe, but also under certain U.S. statutes, direct criminal liability exists, so the consequences of getting it wrong on privacy and data protection issues have increased dramatically.

Implications and Actions

Given the current landscape, certain lessons for businesses and their advisors seem clear:

Follow developments and seek advice regarding evolving legal and regulatory developments.

Designate individuals with responsibility for privacy and data protection strategy, and invest resources in the area. Approach these issues from an interdisciplinary perspective. Legal, marketing, product strategy, IT and development, and other areas each have important responsibilities for privacy and information governance.

Assess and understand how the company plans to collect, use, disclose, and secure data. Issues include what information the company has, what rights it has regarding the data, what it might want to do with the information, where the data might need to move (especially internationally), and how things might be done differently. Additionally, it is increasingly important to understand who will have access to information collected by the business and how long this information will be retained. Many businesses see data as a river to be harnessed for their advantage, but navigating the waters without being perceived as pirates or avoiding running aground can be difficult.

Think about the data supply chain. With “increased accountability” as the new buzzword, enterprises should think about these issues in the context of their vendors, suppliers, and partners. Often the greatest exposures come from outside the business itself.

Evaluate written information-security and incident-response plans. Increasingly, the absence of documented compliance and risk-management protocols may cause businesses to lose sales and face dramatically increased costs, and can jeopardize the existence of the business in a crisis. Not only do privacy and information security often come up in contract negotiations with important customers and suppliers, but when incidents do occur, the presence of clearly defined terms and procedures can greatly simplify the handling and potentially mitigate the damage of a data-related emergency.

Consider privacy and data protection training. The old saying that an ounce of prevention is worth a pound of cure certainly is true in this context. By pushing information out and down within organizations, many significant risks

associated with privacy and data protection issues can be identified and avoided.

The intense current scrutiny of the collection, use, and disclosure of online data and the negative consequences of mistakes and missteps make privacy and information governance an area of critical importance to businesses and their advisors.

Wendell Bartnick

Edward Holman

RockYou Agrees to FTC Settlement after Data Breach and Alleged COPPA Violations

By Wendell Bartnick and Edward Holman

The Federal Trade Commission (FTC) once again has made it clear that companies' data security practices must match their policies. Social gaming company RockYou Inc. allegedly promised that it would take commercially reasonable precautions to safeguard data, but the FTC concluded that the company's precautions did not meet that standard. As a result, RockYou must implement and maintain an information security program and obtain third-party audits for 20 years. Beyond the ongoing program and audits, the FTC also fined RockYou $250,000 for knowingly collecting personal information from children under 13 years of age and not complying with the requirements of the Children's Online Privacy Protection Act (COPPA). This settlement highlights the importance of businesses properly securing the data that they collect online and being aware of what personal information is collected and from whom.

Background

On March 27, 2012, the FTC announced a settlement with RockYou resolving its investigation into alleged misrepresentations of RockYou's information security practices and violations of COPPA.

According to the complaint, RockYou has operated social gaming websites since 2006. To register with the RockYou websites, users enter their email address and password for that email address. Users also can enter their birth year and other information. For about a year, RockYou accepted registrations from approximately 179,000 children under the age of 13. RockYou stored all of this information, including passwords, in clear text. In 2009, RockYou experienced a data breach of approximately 32 million email addresses and RockYou passwords.

In its privacy policy, applicable at the time of the breach, RockYou allegedly promised to use commercially reasonable physical, managerial, and technical safeguards. Further, the policy allegedly stated that RockYou would not knowingly collect personal information from children under 13 and would delete such information upon notice.

Alleged Misrepresentations in RockYou's Privacy Policy

In its complaint, the FTC alleged that RockYou made deceptive claims in its privacy policy, which violated Section 5 of the FTC Act prohibiting "unfair or deceptive acts or practices in or affecting commerce." The FTC claimed that RockYou made deceptive claims when it promised commercially reasonable data safeguards, but that it:

- unnecessarily collected email address passwords and stored them in clear text;
- failed to segment servers, allowing unauthorized users access to the entire computer network;
- left its website vulnerable to common hacking methods; and
- knowingly collected, and did not delete, information about children under 13.

Alleged Collection of Information from Children under 13 Years of Age

COPPA regulates the online collection of personal information from children under 13 years of age, as well as the use and disclosure of such information. It applies to commercial websites and online services that are directed at children or that collect children's personal information with actual knowledge. The operators of these websites and online services may not collect, use, or disclose children's personal information without giving direct notice of their privacy policies to parents and obtaining verifiable consent from them.

The FTC alleged that RockYou knowingly collected personal information from approximately 179,000 children under the age of 13, meaning that RockYou would need to comply with COPPA. The FTC alleged specifically that RockYou violated COPPA by failing to:

- provide on its websites sufficient notice of its information practices;
- provide direct notice to parents of its information practices;
- obtain verifiable consent from parents prior to collecting, using, and disclosing personal information about children; and
- establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of the collected information.

Settlement

The government sought and received several different kinds of relief in the settlement. RockYou may not make deceptive claims about its data security and must establish and implement a comprehensive information security program with biennial independent audits for 20 years. This aspect of the settlement reflects an ongoing trend toward the retention of third-party experts to review privacy practices.

RockYou also agreed to pay a fine of $250,000, delete the children's personal information it collected in violation of COPPA, not commit future violations of COPPA and Section 5 of the FTC Act, and post conspicuous website links to the child-safety website http://onguardonline.gov. These terms are typical components of FTC settlement agreements for COPPA violations.

Implications

The lawsuit and its settlement have important implications for businesses operating websites that may collect personal information from children, especially those that knowingly engage in this practice. If a company's website collects a user's date of birth, the company may be "on notice" of any personal information it collects from children and be subject to COPPA. Complying with COPPA includes publishing and following privacy policies that fully state how the website operator collects, uses, and discloses children's personal information. Further, collection of children's personal information prior to providing direct notice to parents and obtaining their verifiable consent may create significant liability.

Requiring information security programs is a common element in the FTC's other recent information-security-related enforcement actions. This requirement shows the FTC's belief that company-wide information security programs are an effective method for companies to improve the protection of information they collect about consumers. As the FTC stated in its recent final report on privacy,[1] companies should view the privacy and information security programs mandated in these types of orders as roadmaps for their own programs.

[1]Our WSGR Alert discussing the FTC's final report on privacy is available at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-FTC-final-privacy-report.htm.

FTC Releases Final Privacy Report, Sets Forth Best Practices, and Calls for Federal Privacy, Data Security, and Breach Notification Legislation

By Matthew Staples

The Federal Trade Commission (FTC)[1] recently issued a long-anticipated final report on privacy, *Protecting Consumer Privacy in an Era of Consumer Change: Recommendations for Businesses and Policymakers*.[2] The final report comes more than a year after the FTC's preliminary staff report on consumer privacy, which proposed a new framework for addressing privacy issues based upon three general principles: privacy by design, simplified choice, and greater transparency. The final report represents the FTC's view as to best practices regarding consumer data and encourages the adoption of legislation and industry self-regulation.

In its final report, the FTC largely retained its proposed three-principle framework, but it revised its recommendations in three key areas: the scope of

the framework, the contexts in which the framework calls for notice and choice to consumers prior to the collection and use of certain data, and the practices of data brokers. Specifically, the revised recommendations:

- clarify what information may be "reasonably linked to a specific consumer, computer, or other device," thereby falling within the framework, and provide a very narrow exception for small businesses that do not share the information they collect;
- exempt from the notice and choice requirement "practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law"; and

- call for Congress to consider legislation governing the practices of data brokers regarding transparency and consumer control over the information collected.

The report also calls for federal privacy, data security, and data breach notification legislation, and urges industry to accelerate the pace of self-regulation to implement the framework.

Scope of Final Framework

The final framework, like the proposed framework, applies broadly to "all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device." This includes consumer information collected or used both online and offline.[3]

The FTC clarified that data will not be deemed "reasonably linked" to a specific consumer, computer, or device if a company: (1) takes reasonable measures to ensure that the data is de-identified (i.e., the company has a "reasonable level of justified confidence" that the information cannot be used to infer information about or otherwise be linked to a specific consumer, computer, or device); (2) publicly commits to maintain and use the data only in a de-identified manner and not to try to re-identify it; and (3) contractually prohibits downstream data recipients from trying to re-identify the data.

Privacy by Design

The final report retains the FTC's proposed best practice that calls on companies to promote and incorporate substantive consumer privacy protections throughout their organizations and at every step in the process of developing products and services. The FTC indicated that it would like to see substantive protections such as reasonable security for consumer data, reasonable collection limits, sound retention practices, and measures to ensure data accuracy.

The report calls upon industry to develop and implement "best data security practices" for industry sectors and types of consumer data not addressed presently by self-regulation. It also calls upon Congress to enact data security and breach notification legislation authorizing the FTC to seek civil penalties for violations.

Regarding reasonable limits on data collection, the final report clarifies that, under the framework, companies should limit data collection to what is consistent with the context of the transaction or the relationship between the company and consumer, or what is required or specifically authorized by law. Where the collection would be inconsistent with consumer expectations at the time of collection, companies should provide prominent notice and choice to the consumer outside of a privacy policy or other legal document. The framework requires companies to determine the purpose of any data collection prior to it taking place, and to not collect data for possible future purposes. Companies also should satisfy their business purposes by collecting data that has the minimum potential privacy implications.

With respect to data retention, the final report continues to set forth a best practice of limiting data retention and disposing of it once it outlives the purpose for which it was collected. Declining to define a specific data retention period as a best practice, the report instead calls for flexible procedures commensurate with a company's size and the risks associated with the data it collects, uses, and maintains.

The final framework continues to ask companies to take reasonable steps to ensure the accuracy of the data collected and maintained, particularly where the data could be used to cause significant harm or to deny services to consumers. The framework adopts a flexible approach, calling for different requirements depending upon the intended use and sensitivity of the data. Under this approach, companies using consumer data for marketing purposes need not take special measures to ensure the accuracy of such data. Companies using the data to determine a consumer's eligibility for benefits, however, should take measures to ensure accuracy, including giving consumers access to the data and providing an opportunity to correct it.

To implement these best practices, the final report continues to encourage companies to adopt and maintain comprehensive data-management procedures throughout their product or service lifecycles. These procedures may include designating privacy personnel responsible for training employees regarding privacy practices and conducting regular privacy assessments.[4]

Simplified Choice

The FTC retained simplified choice as a core component of its privacy framework. Under the FTC's revised principle, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction or the company's relationship

with the consumer, or when the collection or use is required or expressly authorized by law.

The FTC specifically identified the sale of consumer information to a third party and the tracking of consumers across third-party websites as practices that *would* require notice and choice under the framework. The final report retains the notion that companies should provide notice and choice, when required, at a time and in a context in which the consumer is making a decision about his or her data. It clarifies, however, that precisely how companies achieve these goals practically may vary based on the circumstances. In some instances, notice and choice may be provided *after* data has been collected.[5]

The report endorses obtaining affirmative, express consent from consumers before collecting sensitive data, such as information about children, finances, or health, regardless of the use of such data.[6] Similarly, the report states that companies should obtain affirmative, express consent before making material, retroactive changes to privacy representations. For the consumer's choice to be meaningful, the framework rejects a "take it or leave it" approach for important services where consumers have few options, such as broadband access.

The final report continues to advocate for the implementation of a "Do Not Track" mechanism that would give consumers choice with respect to online behavioral tracking.

Greater Transparency

The report reaffirms the FTC's proposed principle that companies should make privacy policies clearer, shorter, and more uniform so that consumers, regulators, and others may more easily compare policies among different companies. The FTC believes that uniformity can be achieved by industry sector.

The report also reaffirms the FTC's position that companies should provide consumers with reasonable access to data maintained about them. For data maintained for marketing purposes, the FTC concluded that the cost of providing individualized access and correction rights likely would outweigh the benefits. It did, however, endorse the practice of companies giving consumers access to a list of categories of data they hold, and the ability to opt out of its use for marketing. In contrast, businesses maintaining consumer data for use by creditors, employers, insurance companies, and others that make eligibility determinations with the data should provide consumers with access to their data and the ability to correct erroneous information. For companies that lie somewhere in the middle, the report endorses a sliding-scale approach; companies should adjust consumers' ability to access data about them based on the use and sensitivity of the data. The report asserts that, at minimum, companies should offer consumers access to (1) the types of information companies maintain about them and (2) the sources of such information.

Next Steps

The FTC's report calls for federal legislation in multiple areas and urges industry to accelerate the pace of self-regulation. It also identifies five areas in which the FTC will focus its policymaking efforts this year:

- *Do Not Track*. The FTC intends to work with industry, browser vendors, the Digital Advertising Alliance, and the World Wide Web Consortium to implement an easy-to-use, persistent, and effective "Do Not Track" system.
- *Mobile*. The FTC will update its business guidance about online advertising disclosures to help companies with mobile services provide short, meaningful disclosures to consumers.
- *Data Brokers*. Of particular concern to the FTC are data brokers that combine consumer data from several sources and resell it, often without the consumer's knowledge. The FTC will advocate for targeted legislation requiring data brokers to provide consumers with access to information the broker holds about them. Further, the FTC recommends the creation of a centralized website where data brokers that use data for marketing can identify themselves to consumers and describe how they collect and sell consumer data. The website also could educate consumers on their access rights and provide links to exercise those rights.
- *Large Platform Providers*. The FTC will host a public workshop to better understand how Internet service providers, operating systems, browsers, and social media companies track consumers' online activities comprehensively.
- *Enforceable Self-Regulatory Codes*. The FTC will participate in the Department of Commerce's project to facilitate the development of sector-specific, voluntary codes of conduct.[7]

Implications

The FTC's privacy framework is likely to have a significant impact on consumer data collection and use practices in all sectors of the economy. The FTC made clear in its report that, to the extent the framework goes beyond existing legal requirements, it is not intended to serve as a template for law-enforcement actions or regulations under laws the FTC currently enforces. The report does, however, urge industries to adopt self-regulatory codes of conduct implementing the framework, and states that the FTC will take enforcement action against companies that fail to abide by any self-regulatory programs they join.

Regardless of whether companies are bound formally by the framework, they should think carefully, and early on, about information governance strategy, especially where a business model depends upon or requires data monetization.

[1] The FTC is the nation's leading consumer protection enforcement agency and has the authority to regulate all unfair and deceptive trade practices occurring in interstate commerce. The FTC has used this authority to

assert jurisdiction over privacy-related matters for most businesses.
[2] The final report, released on March 26, 2012, is available at http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[3] In recognition that the framework may place an undue burden on small businesses, it does not apply to companies that (1) collect only non-sensitive information from fewer than 5,000 consumers a year and (2) do not share it with third parties.
[4]The final report recommends a reasonable transition period for companies to update legacy systems to incorporate the privacy framework. It suggests that companies update systems with sensitive data first and appropriately limit access to such systems until they are updated.
[5]For example, the report commends the online behavioral advertising industry's development of a standardized icon and text that is embedded into targeted advertisements because the in-ad disclosure provides a logical "teachable moment" for the consumer.
[6] The FTC declined to require affirmative, express consent for the collection of data about users between the ages of 13 and 17, but recommended that companies that target teens consider additional protections, such as shorter retention periods for teens' data. The FTC also stated that social networking sites should consider implementing more privacy-protective default settings for teen users.
[7] For background on the Department of Commerce's privacy framework, including its efforts to facilitate the development of voluntary codes of conduct relating to consumer privacy, please see the WSGR Alert at http://www.wsgr.com/WSGR/Display.aspx?SectionName=publications/PDFSearch/wsgralert-consumer-privacy-bill-of-rights.htm. The FTC noted in its final report that staff from the FTC and the Department of Commerce sought to ensure that the agencies' privacy initiatives are complementary, and that the agencies will continue to work collaboratively to guide the implementation of their respective privacy initiatives.

Donald Vieira

Brock Dahl

The Cybersecurity Act of 2012: Senate Proposes a New Regulatory Regime to Protect Critical Infrastructure

By Donald Vieira and Brock Dahl

Over the past few years, numerous cybersecurity proposals have emerged on Capitol Hill that would impact the activities of the private sector if passed into law. One recent proposal, the Cybersecurity Act of 2012,[1] has the support of the Obama Administration and has rejuvenated the effort to pass cybersecurity legislation on the Hill. The act proposes a new and highly significant regulatory framework for governing private-sector cybersecurity practices: a mandatory compliance regime covering certain sectors of the economy and a voluntary compliance regime that would encourage other private-sector entities to organize and share information regarding the cyber threat. These proposed regimes, and the private-sector reaction to them, are playing a significant role in shaping the move toward greater codification of corporate responsibility to secure cyberspace.

This article briefly describes the two proposed regimes and focuses on the issues they raise for private-sector companies.

Mandatory Compliance

As noted above, the Cybersecurity Act includes a regulatory compliance regime that would be mandatory for a certain subset of the American economy. It would empower the Secretary of Homeland Security to establish a mandatory compliance regime designed to protect “Covered Critical Infrastructure.” The Cybersecurity Act defines “critical infrastructure” as encompassing systems and assets whose destruction would have a “debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”[2] The act gives the Secretary authority to determine which sectors, systems, or assets fall under this regime, with certain limitations.[3] For example,

covered infrastructure cannot include information technology products or services solely because they are *used in* Covered Critical Infrastructure, and the infrastructure also cannot include "commercial information technology" products—a carve-out that would seem to exclude standard consumer electronics products from the purview of the mandatory compliance regime.[4]

Under the proposed regime, once a sector, and presumably a system or asset within the sector, is determined to be Covered Critical Infrastructure, it will be subject to certain security requirements and reporting obligations. Under the Cybersecurity Act, federal regulations are to be promulgated mandating satisfaction of the requirements. The act establishes a procedure whereby the Secretary of Homeland Security develops those regulations following a process that includes statutorily mandated input from the private sector. The act states that the Secretary is to perform sector-by-sector risk assessments "in consultation with" a range of private and government entities. The risk assessment will help the government prioritize key sectors for further analysis and potential regulation.[5] The Secretary also will consult with the same private-sector group to develop security performance requirements that would serve as the basis of the Secretary's regulations.[6] Ultimately, covered parties would be required to inform the Secretary and any other relevant federal agency[7] of the security measures that it has selected to satisfy the requirements.[8] In addition, covered parties must either certify annually that they have met the performance requirements established by the regulations or submit third-party assessments to that effect.[9] Finally, there is a requirement that covered parties report significant cyber incidents to the government.[10]

Voluntary Compliance

A second section of the Cybersecurity Act encourages information sharing and heightened cybersecurity activities by all other private entities. Unlike the mandatory compliance regime, the Cybersecurity Act merely encourages information sharing by this broader group.[11] It does so primarily by creating cybersecurity exchanges that will facilitate the provision of certain threat information from the government to the private sector.[12] The Cybersecurity Act encourages private entities to disclose threat information to cybersecurity exchanges and, as in the mandatory regime, offers certain protections against the public disclosure and certain potential uses of the information that is provided to the exchange.[13]

Incentives for Private-Sector Entities to Monitor and Report

The drafters of the legislation, responding to concerns raised by the private sector over the information-disclosure requirements contained in the act, included provisions intended to mitigate the risk of information disclosure and provide incentives for companies to report cyber concerns. These provisions offer certain liability protections when a company has complied with the reporting

requirements, and also place limitations on the public disclosure or utilization of information that has been provided to government agencies.[14]

In addition, the Cybersecurity Act allows for certain monitoring by the private sector of third-party systems when authorized.[15] The act limits private-sector civil and criminal liability for such measures and the disclosure of certain information to the government that was obtained legally.[16] It also permits a "good faith" defense against certain civil and criminal actions in which the party relied in good faith on a belief that its actions were permitted by the Cybersecurity Act.[17] Finally, information provided pursuant to certain sections of the act cannot be used in regulatory actions against the private-sector entity that disclosed the information.[18]

Moving Forward: Issues for Consideration

The public's reaction to the Cybersecurity Act has highlighted several issues with the legislation that likely will receive significant attention if the bill moves toward consideration by the full Senate. First, there are concerns from private-sector companies and civil liberties groups about the nature of the information that the regulations will require companies to report to the government. The private sector's concerns are focused on the burden of the requirements, as well as the safety and confidentiality of information it provides. Ultimately, the private sector is worried about disclosing proprietary information to the government and the potential for creating legal, competitive, and security vulnerabilities if that information is not properly managed. Meanwhile, the civil liberties community is focused on what it considers the use of broad definitions for certain key terms in the act and the possibility that these broad terms may increase the government's authority to monitor individuals or organizations. For example, the Cybersecurity Act proposes "cybersecurity threat indicators" as the primary type of information to be provided to the government. The civil liberties community is concerned that this term has a potentially broad meaning, and that it is not clear exactly what this encompasses, how much detailed information on individuals and organizations could be disclosed, or what exactly the government can do with the information once it is provided.

In the end, it is the very existence of a mandatory compliance regime that is generating the most debate on the Hill. The primary counterproposal in the Senate to the Cybersecurity Act, the "SECURE IT" Act (known as the "Secure Act"), put forth in March 2012,[19] does not contain a mandatory compliance regime. Instead, rather than protecting critical infrastructure through direct regulation as the Cybersecurity Act attempts to do, the Secure Act provides for criminal penalties for damage to certain critical infrastructure.[20] This substantive difference highlights the divergent viewpoints about mandatory compliance and illustrates that a significant legislative compromise still is required to reconcile the Senate's view on what a cybersecurity law should include.

Thus, the nature of mandatory versus voluntary compliance relationships, the type of information that will be provided to the government, and how the

government will store, process, and protect such information remain under debate. Nonetheless, the Cybersecurity Act of 2012 provides a likely baseline from which revisions and new proposals will emerge, and we expect it to receive additional attention and support as Congress moves toward passing cyber legislation.

[1]Cybersecurity Act of 2012, available at http://www.hsgac.senate.gov/download/the-cybersecurity-act-of-2012-s-2105 (last accessed April 9, 2012).
[2]The Cybersecurity Act cites the USA Patriot Act, 42 U.S.C. 5195(c)(e), for this definition.
[3]Cybersecurity Act Section 2(3) and 103.
[4]Cybersecurity Act Section 103(b)(2)(B)-(D), utilizing the definition of "commercial item" at 41 U.S.C. 103 to exclude such items from the definition of covered infrastructure.
[5]See generally, Cybersecurity Act Section 102.
[6]Cybersecurity Act Sections 104(b)(1) and 105(b)(1)-(2).
[7]The act provides that the federal agency with primary responsibility for the security of the covered sector may enforce the regulations promulgated by the Department of Homeland Security (DHS), but also includes provisions allowing DHS to enforce regulations directly under certain circumstances.
[8]Cybersecurity Act Section 105(b)(2).
[9]Cybersecurity Act Section 105(c).
[10]Cybersecurity Act Section 105(b)(1)(D).
[11]Cybersecurity Act Section 707(e).
[12]See generally Cybersecurity Act Section 703.
[13]See Cybersecurity Act Section 704(d), (e), and (f).
[14]Cybersecurity Act Section 105(e)(1)(A)-(C); 107(b), citing the Homeland Security Act (6 U.S.C. 133).
[15]See generally Cybersecurity Act Section 701.
[16]See Cybersecurity Act Section 706 (a)(1) and (2).
[17]Cybersecurity Act Section 706(b).
[18]Cybersecurity Act Section 706(c).
[19]The "Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012" is available at http://commerce.senate.gov/public/?a=Files.Serve&File_id=e1244f6d-24ac-44b0-872e-61e1ce6509e6 (last accessed April 9, 2012).
[20]Secure Act Section 305.

Marina Tsatalis

Rebecca Stuart

To Ask or Not to Ask: Can Employers Demand Social Media Passwords from Employees and Applicants?

By Marina Tsatalis and Rebecca Stuart

Recently, the Internet has been buzzing with renewed interest in the employer practice of asking current employees and applicants to divulge their social media passwords to enable employers to review social media profiles for suspicious or inappropriate activity. While this is an issue that has been discussed in legal circles for many years, a recent spike in interest by the media, advocacy groups, legislators, and the general public has refocused attention on the subject, which strikes at the core of individual privacy rights and the bounds of an employer's ability to access the social media information of its current and prospective employees.

The recent increase in exposure can be traced partially to a 2010 incident in which the Maryland Division of Corrections demanded Facebook log-in credentials from a corrections officer, Robert Collins, following his return from leave.[1] Mr. Collins was not, however, the first employee to be subject to such a request by a government agency. Since 2006, the sheriff's office of McLean County, Illinois, has requested social media log-in information from all job applicants.[2] In 2009, the City of Bozeman, Montana, required all applicants to

provide social media log-in information, though the practice has since been discontinued.[3] In 2011, a teacher's aide at Frank Squires Elementary in Cassopolis, Michigan, was fired when she refused to provide her employer with her Facebook log-in information, including her password.[4]

While law enforcement and government agencies have achieved the most notoriety for demanding social media credentials from current and prospective employees, private employers are not immune from such scrutiny. Most recently, a New York City statistician withdrew his application from a private company when he was asked for his social media password during the interview.[5]

On March 23, 2012, Facebook issued a statement condemning the practice of requesting social media log-in information from job applicants, stating in part, "This practice undermines the privacy expectations and the security of both the user and the user's friends. It also potentially exposes the employer who seeks this access to unanticipated legal liability."[6] In addition, Facebook has made it a violation of the company's Statement of Rights and Responsibilities to share or solicit a Facebook password.

But is asking for social media credentials actually illegal? Federally, the answer appears to be unsettled. On March 26, 2012, New York Senator Charles Schumer and Connecticut Senator Richard Blumenthal asked the U.S. Department of Justice to investigate whether the practice violates existing federal law.[7] As their basis for believing requests for social media passwords are illegal, the senators cited the Stored Communications Act (SCA),[8] which protects individuals against unauthorized disclosure of electronic communications, and the Computer Fraud and Abuse Act (CFAA),[9] which protects individuals from intentional access by a third party to a computer without authorization.

To further bolster their position, the senators cited *Pietrylo v. Hillstone Restaurant Group*,[10] a 2008 federal trial court case in New Jersey. In *Pietrylo*, the plaintiffs were restaurant employees who belonged to an invitation-only, password-protected chat group. A manager obtained access to the group from one of the invited employees, and the plaintiffs brought suit claiming a violation of the SCA. The court ultimately agreed that the SCA was violated, finding the restaurant's argument that access to the website was "authorized" unpersuasive—the court instead found that a jury could conclude that the "purported authorization was coerced or provided under pressure."[11] Expanding *Pietrylo* to the current debate would mean that even if an employee provides his or her employer with log-in information for a social media site, the employer's use of that information still may be unauthorized and a violation of the SCA. This argument is strengthened by the current economic downturn—an applicant may feel that he or she has no choice but to accept an employer's precondition or remain unemployed. The *Pietrylo* decision has limited impact, however, as it is not binding on any other state or federal courts. Specifically, there is no requirement that the federal government follow *Pietrylo* in resolving the current

debate over requesting social media passwords from current or prospective employees.

In a further attempt to secure federal protections against employers asking for social media credentials, Democratic lawmakers in Congress inserted an amendment into a Federal Communications Commission bill that would prohibit the practice of requesting passwords from applicants.[12] On March 27, 2012, the measure was blocked primarily along party lines, with the chairman of the Energy and Commerce Subcommitte on Communications and Technology, Representative Greg Walden (R-Oregon), indicating that the amendment does not protect privacy, as the Democrats claimed.[13]

In the absence of a clear federal law prohibiting the practice of asking for applicants' or employees' social media passwords, some states are stepping in to fill the void. On April 11, 2012, Maryland became the first state to pass a law prohibiting employers from requesting or requiring social media account information from current or prospective employees.[14] On April 24, 2012, California's version of a similar bill easily passed through an early committee with the support of both labor groups and business lobbies, and it is poised to move into the next round of the legislative approval process.[15] The bill, similar to Maryland's new law, would prohibit employers from requiring a prospective or current employee to disclose his or her social media account information.[16] Similar proposed laws currently are pending in Minnesota,[17] Washington,[18] Illinois,[19] and New York,[20] among other states.

While Maryland and California are passing laws specifically relating to employers requesting social media credentials from applicants and employees, California has an existing law relating to employee privacy that may cover these types of requests. In an attempt to prevent pre-employment discrimination, a California regulation specifically prohibits an employer from requesting a photograph of an applicant or making any type of request that would identify the applicant, directly or indirectly, on any basis protected under California's Fair Employment and Housing Act.[21] Requesting a social media password could be viewed as a way of avoiding liability under the regulation, while effectively gaining the same end-product since most applicants and employees have photographs of themselves on their social media pages.

Consequently, state and perhaps federal law eventually may prohibit some employers from asking for social media log-in information, but in the meantime the practice is not strictly prohibited in most states. This raises the question: if employers *can* ask for social media passwords, *should* they? In most cases, the answer is no. Information obtained from social media websites may well put the employer on notice about certain aspects of a prospective employee that the company would rather not know prior to making a hiring decision, including the employee's race, sex, disability status, and sexual orientation. Additionally, best practices for gathering information about employees include limiting the information sought to only that which is related to the job at issue, including whether the individual is capable of performing the duties of the position. Traditional interviews, reference checks, and background checks will tend to be

sufficient in most cases. Furthermore, given the current backlash against employers that request or require social media credentials from current or prospective employees, companies that make such a request may be subject to a public relations problem, or may face a morale issue within their organizations.

As the law applicable to social media continues to evolve, employers will continue to face challenges related to what they can ask an employee, and what employee or applicant information they can view online. Staying up-to-date on current developments and obtaining the assistance of a knowledgeable employment attorney will help employers navigate the potential pitfalls of this complicated topic.

[1] Emil Protalinski, "Employer Demands Facebook Login Credentials During Interview," ZDNet.com, Feb. 20, 2011, http://www.zdnet.com/blog/facebook/employer-demands-facebook-login-credentials-during-interview/327?tag=mantle_skin;content; Manuel Valdez, "Job Seekers Getting Asked for Facebook Passwords," Time.com, March 20, 2012, http://techland.time.com/2012/03/20/job-seekers-getting-asked-for-facebook-passwords/ (cited hereafter as "Job Seekers").
[2] Job Seekers.
[3] Job Seekers.
[4] Michael Santo, "List of Employers Demanding Facebook Passwords Continues to Grow," Examiner.com, April 2, 2012, http://www.examiner.com/technology-in-national/list-of-employers-demanding-facebook-passwords-continues-to-grow.
[5] Job Seekers.

[6] Erin Egan (Chief Privacy Officer, Facebook), "Protecting Your Passwords and Your Privacy," "Facebook and Privacy" page, http://newsroom.fb.com/Announcements/Protecting-Your-Passwords-and-Your-Privacy-134.aspx.
[7] David Cohen, "More Lawmakers Champion Facebook Password Privacy," AllFacebook.com, March 26, 2012, http://allfacebook.com/facebook-password-privacy_b83269.
[8] 18 U.S.C. §§ 2701-2712.
[9] 18 U.S.C. § 1030.
[10] 2009 U.S. Dist LEXIS 88702 (D.N.J. Sept. 25, 2008).
[11] 2009 U.S. Dist LEXIS 88702 (D.N.J. Sept. 25, 2008).
[12] Sam Favate, "House GOP Says 'Not So Fast' to Bill on Facebook and Job Applicants," *Wall Street Journal*, March 28, 2012, http://blogs.wsj.com/law/2012/03/28/house-gop-says-not-so-fast-to-bill-on-facebook-and-job-applicants/?mod=WSJBlog (cited hereafter as "House GOP").
[13] House GOP.
[14] SB 433 and HB 964.
[15] Maria Noel Fernandez, "Social Media Privacy Bill Receives Unanimous Support," *Assembly Member Nora Campos' Website*, April 24, 2012, http://asmdc.org/members/a23/component/k2/item/2650-social-media-privacy-bill-receives-unanimous-support.
[16] AB 1844, introduced by Assembly Member Nora Campos, February 22, 2012.
[17] HF 2963, introduced March 26, 2012.
[18] SB 6637, introduced April 6, 2012.
[19] HB 3782, introduced by Representative LaShawn K. Ford, May 18, 2011.
[20] SB 6938, introduced April 13, 2012.
[21] Cal. Code Regs. tit. 2 § 7287.3(c)(2) (2009).

Supreme Court Favors First Amendment Right to Use Data Obtained During Commercial Transactions for Targeted Marketing over Privacy Concerns

By Tonia Klausner

Last June, the United States Supreme Court struck down on First Amendment grounds a Vermont law prohibiting the sale or use of certain data for marketing purposes (*Sorrell v. IMS Health*, 131 S. Ct. 2653 (2011)). Although the decision

received little media attention, it could be of significant benefit to companies engaged in targeted advertising.

The law at issue addressed a marketing practice engaged in by pharmaceutical companies called "detailing," whereby the companies send sales representatives to doctors' offices to try and persuade the doctors to prescribe particular drugs. In order to target the doctors who are likely to be the most interested in prescribing a particular drug, the pharmaceutical companies obtain information about doctors' prescription practices—"prescriber-identifying information"—from data-mining companies. The data miners, in turn, purchase the data from pharmacies that have obtained it through the ordinary course of their business operations. Vermont passed a law that generally prohibited the sale, license, or use of such prescriber-identifying information for the purposes of marketing or promoting a prescription drug, absent the prescriber's consent. In a six-to-three decision, the Supreme Court held that the law did not pass constitutional muster.

The Supreme Court's Decision

The Court first concluded that marketing is a form of protected speech—"speech with a particular content." Because the law prohibited the use of information for marketing purposes, the Court found it to be content-based. Because it was directed at pharmaceutical manufacturers, it also was speaker-based. With this premise, the Court went on to apply heightened judicial scrutiny to the law to determine whether it directly advanced a substantial governmental interest and was drawn to achieve such interest. In doing so, the Court rejected the state's argument that heightened scrutiny was not appropriate because the law was merely a commercial regulation with an incidental impact on speech. Rather than imposing merely an incidental burden, the Court found the law to be directed at a specific type of content and speaker. The Court also rejected the state's argument that the law merely regulated access to information subject to state regulation. The Court found of particular significance the fact that the data at issue was already in the hands of private entities. It further rejected the state's position that the law regulated conduct—the sale, transfer, and use of information as a commodity—rather than speech. According to the Court, the creation and dissemination of information are speech, whether that information is on a beer label, in a credit report, or in a prescription record.

Lastly, the Court concluded that neither of the two justifications for the law advanced by the state—privacy and improved healthcare—withstood scrutiny. The state argued that doctors have a reasonable expectation that their prescription information will not be used for any purpose other than to fill prescriptions. It further argued that the law protected doctors from "harassing sales behaviors." As to the first privacy concern, the Court concluded that even if legitimate, the law was not drawn to directly serve that purpose because the data at issue could be sold and used for non-marketing purposes. Meanwhile, the Court rejected the second concern outright, stating that "[m]any are those who must endure speech they do not like, but that is a necessary cost of freedom." The Court recognized the state's legitimate interest in lowering the

costs of medical services and promoting public health, but concluded that the law did not directly advance these interests.

Implications

Companies in the targeted advertising space should see this opinion as a ray of hope in the otherwise currently bleak landscape of viewpoints on behavioral advertising. Congress, the FTC, privacy advocates, and the plaintiffs' class action bar all have attacked the practice of targeted advertising based on data about Internet and mobile device users' behavior collected in the ordinary course of business as offensive to consumers' privacy interests. The Supreme Court's ruling suggests that any law specifically intended to preclude targeted advertising based on data collected during the ordinary course of business and then sold through data brokers or otherwise could run afoul of the First Amendment.
