

ADVISORY

SULLIVAN & WORCESTER LLP PRIVACY & DATA SECURITY ADVISORY

Privacy & Data Security Law Developments: 2010 Mid-Year Update

This first half of 2010 has, as predicted, seen significant attention given to privacy issues by Congress, regulatory agencies, and the courts. In this Advisory, we provide a mid-year summary of significant developments in each of the five subject matter areas covered by the Sullivan & Worcester Privacy & Data Security practice group's multi-disciplinary team.

PRIVACY OF CONSUMER INFORMATION AND COMPLIANT MARKETING PRACTICES

- On July 19, 2010, Rep. Bobby Rush (D-Ill.), Chairman of the House Commerce Subcommittee on Commerce, Trade, and Consumer Protection ("Subcommittee"), introduced the "[Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguard Act](#)," or the "BEST PRACTICES Act." The Subcommittee held a hearing on the BEST PRACTICES Act and the draft [Boucher-Stearns privacy bill](#). The Boucher-Stearns bill, a draft of which was released on May 3, 2010 (but has not been formally introduced) is similar in intent to the BEST PRACTICES Act. Both bills have drawn significant criticism from the business community, with some prominent commentators contending that the bills' consumer privacy protections will slow e-commerce to a crawl.

The Subcommittee's [Briefing Memo](#) prepared for the July 22 hearing notes a series of high-profile privacy lapses to which the proposed consumer privacy bills are addressed: Google's launch of its social network service Google Buzz; changes to Facebook users' privacy settings; the collection of payload data from open WiFi networks by Google's Street View cars; and Sears' collection of highly-sensitive personal information via a downloadable software application.

The Act proposes a bevy of new regulations to be administered by the Federal Trade Commission, with penalties for non-compliance reaching \$5 million, and a limited private right of action provided. The regulations would require all businesses (with a limited exemption for small businesses storing information from or about less than 15,000 individuals) to provide to individuals details about the companies' privacy practices, including a description of the information collected and the specific purposes for such collection. Individuals could opt out of the collection and use of their

IF YOU WOULD LIKE ADDITIONAL INFORMATION, PLEASE CONTACT:

David A. Guadagnoli
617 338 2938
dguadagnoli@sandw.com

Kimberly B. Herman
617 338 2943
kherman@sandw.com

Ilene Robinson Sunshine
617 338 2928
isunshine@sandw.com

Kathy L. Cooper
202 370 3926
kcooper@sandw.com

Kristen D. Danaher
617 338 2489
kdanaher@sandw.com

Amy E. Sheridan
617 338 2897
asheridan@sandw.com

Christopher T. Stevenson
617 338 2428
cstevenson@sandw.com

Ronald P. Whitworth
202 775 1219
rwhitworth@sandw.com

BOSTON

Sullivan & Worcester LLP
One Post Office Square
Boston, MA 02109

NEW YORK

Sullivan & Worcester LLP
1290 Avenue of the Americas
New York, NY 10104

WASHINGTON, DC

Sullivan & Worcester LLP
1666 K Street, NW
Washington, DC 20006

ISRAEL

Zysman, Aharoni, Gayer and
Sullivan & Worcester LLP
41-45 Rothschild Blvd., Beit Zion
Tel Aviv, 65784 Israel

SULLIVAN &
WORCESTER

information, and the bill would require covered entities to obtain express affirmative opt-in consent before collecting, using, or disclosing "sensitive information" including information concerning:

- medical history;
- race or ethnicity;
- religious beliefs and affiliation;
- sexual orientation or sexual behavior;
- financial information;
- precise geolocational information (and any information about the individual's activities and relationships associated with such geolocation);
- unique biometric data; and
- social security numbers.

The bill also includes data security, access, data minimization, accountability, and accuracy requirements.

- On July 27, 2010, the Senate Committee on Commerce, Science, and Transportation held a hearing on [Online Consumer Privacy](#) at which the Committee took testimony from witnesses representing Google, AT&T, the Federal Trade Commission ("FTC"), the Federal Communications Commission ("FCC"), and various think tanks, among others. Speaking of "ordinary Internet users," Committee Chairman Jay Rockefeller said in a written statement: "We have a duty to ask whether these people – and the millions of Americans just like them – fully understand and appreciate what information is being collected about them, and whether or not they are empowered to stop certain practices from taking place."
- In June, the [Supreme Court of California](#) held that an allegedly misleading and deceptive e-mail marketing practice was in fact compliant with California law. According to class action plaintiff Craig E. Kleffman, he received 11 unsolicited email advertisements for Vonage's broadband telephone services using 11 different domain names: superhugeterm.com; formycanpansite.com; ursunrchcntr.com; urgtrquirkz.com; countrfolkgoepel.com; lowdirectsme.com; yearnfrmore.com; openwrldkidz.com; ourgossipfrom.com;

specialdlvrguide.com; and struggletailssite.com. Each domain name was traced to a single physical address in Nevada, where Vonage's marketing agent is located. Kleffman claimed that these "random," "varied," "garbled," and "nonsensical" domain names were used to deliberately trick his spam filters into thinking there were multiple senders of the emails, in violation of California Business and Professions Code §17529.5(a)(2), which states that it is unlawful to advertise in a commercial email if the email "contains or is accompanied by falsified, misrepresented, or forged header information."

The Court disagreed, holding that "a domain name in a single email that does not identify the sender, the merchant-advertiser, or any other person or entity simply does not make any 'representation' regarding the e-mail's source, either express or implied, within the common understanding of that term, so it cannot be said to constitute 'misrepresented' information." The Court also found that the California state legislature did not intend §17529.5(a)(2) generally to prohibit the use of multiple domain names.

While the decision is an interesting one, companies engaged in national/international marketing should avoid drawing broad conclusions from the case, as it sets precedent only for the state of California.

PRIVACY OF HEALTHCARE INFORMATION

- The U.S. Department of Health and Human Services ("HHS") has released a Notice of Proposed Rulemaking proposing modifications to rules implementing the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by last year's Health Information Technology for Economic and Clinical Health Act ("HITECH Act"), in anticipation of broader use of electronic health records. Although the underlying statutory provisions that the new rules implement are generally effective February 18, 2010, the proposed rules will generally not be effective for 180 days after publication of the final rules. In addition, the proposed rules provide up to an additional year in which to amend business associate agreements. (The rules published last year relating to notification of data breaches pursuant to HIPAA were not changed by these new rules and remain effective as interim guidance.

Proposed final breach notification rules were expected to be released soon, but HHS recently announced that “given the Department’s experience to date in administering the [rule]” it had removed those final regulations from administrative review to allow for further consideration.)

The HITECH Act and the new rules would enhance the protection of protected health information (“PHI”) subject to HIPAA while expanding enforcement of HIPAA’s Privacy, Security, and Enforcement Rules by:

- enhancing individuals’ rights to access their PHI and restrict certain types of disclosures of PHI to health plans;
- extending the coverage of HIPAA’s Security and Enforcement Rules, certain portions of the Privacy Rule, and the penalty provisions directly to business associates of covered entities;
- implementing the expanded penalty enforcement regime;
- establishing new limitations on the use and disclosure of PHI for sale, marketing, and fundraising purposes;
- explicitly prohibiting the sale of PHI without patient authorization; and
- making a number of other tweaks to existing rules.

In an attempt to ensure that various parties dealing with PHI are subject to these rules, HHS is proposing to expand the definition of business associates to include “subcontractors” of business associates (that is, persons that perform functions for or provide services to business associates and in doing so need access to PHI). One result of this proposed change is to create direct liability under HIPAA for these organizations in the event of noncompliance.

Notices of Privacy Practices will also need to be updated.

The deadline for commenting on the proposed rules is September 13, 2010. Please contact us if we can assist you in preparing and filing comments.

PRIVACY OF FINANCIAL INFORMATION

- [The Data Security Act of 2010](#) (“Data Security Act”), introduced by Sens. Tom Carper (D-Del.), and Bob Bennett (R-Utah), would impose duties on all entities handling sensitive financial information, with a view toward preventing identity theft. The bill, which was originally introduced in 2007 but not passed, would complement the Gramm-Leach-Bliley Act in regulating the responsibility of covered entities to “implement, maintain, and enforce reasonable policies and procedures to protect the confidentiality and security of sensitive account information and sensitive personal information which is maintained or is being communicated by or on behalf of a covered entity.”

Importantly, the Data Security Act proposes uniform procedures to handle the breach of sensitive information across multiple jurisdictions. While nearly every state in the U.S. has a data breach notification law, each is unique and imposes different requirements, making it difficult for covered entities to manage their regulatory responsibilities when a breach occurs. The Data Security Act would preempt these state laws, providing a single, uniform data breach notification standard.

WORKPLACE PRIVACY

- Last month, the U.S. Supreme Court released its opinion on a case that the privacy community anticipated might provide guidance on the extent of employees’ privacy rights when using employer-provided devices. Instead, in [City of Ontario v. Quon](#), the Supreme Court declined to tackle the issue. The Court reversed the decision of the Ninth Circuit, determining, on the facts of this case, that a search of a police officer’s text messages on his work-issued mobile phone did not violate the officer’s Fourth Amendment rights as a public sector employee. But the Supreme Court’s decision was resolved on narrow grounds, with the Court passing on the opportunity to establish precedent on the extent to which the Fourth Amendment may protect the privacy of public sector employees. In declining to weigh in on the ultimate issue, the Court cited rapid changes in technology

and evolving notions of what society deems proper behavior, stating "it is uncertain how workplace norms, and the law's treatment of them, will evolve." For the moment, however, the decision reinforces the need for employers to have clear and consistent policies in place as to how employer-provided devices may be monitored. Simultaneously, the decision puts employees on notice that communications using work-issued devices may not be kept private.

BREACH MANAGEMENT AND LITIGATION

- Pursuant to President Barack Obama's cyberspace policy initiative, the White House National Security staff released the first draft of its "[National Strategy for Trusted Identities in Cyberspace](#)" in June, with a final draft to be issued later this year. The National Strategy was developed to increase the level of trust associated with identities in cyberspace by building a comprehensive "Identity Ecosystem Framework" that will facilitate trust between individuals, organizations, services, and devices through security and authentication of digital identities across multiple platforms. The plan seeks interoperability between platforms such that individuals will have fewer usernames and passwords to manage for various services. The system would be designed to minimize the amount of information transmitted for each transaction. By reducing the disclosure of excess personal information, the plan seeks to lessen the risk of online fraud and cybercrimes.

Following the issuance of the final plan, the White House plans to designate a lead federal agency to coordinate the implementation of the plan, working closely with the Office of the Cybersecurity Coordinator within President Obama's office. The plan is expected to lead to the mandatory adoption of Fair Information Practice Principles ("FIPPs"). FIPPs are a widely-accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that impact individual privacy, including: transparency; individual participation; purpose specification; data minimization; use limitation; data quality and integrity; security; accountability; and auditing. This effort is another example of a continuing trend – the transformation of what

are currently data handling "best practices" into enforceable legal requirements. Clients unsure whether their data handling practices are adequate to meet current and upcoming standards are encouraged to set up an appointment with their S&W Privacy & Data Security attorney to identify any potential problem areas that should be addressed.

- A [proposed settlement](#) between Twitter and the FTC last month highlighted the need for companies to pay close attention to their administrative controls and username/password policies. The FTC issued a complaint against Twitter based on a series of 2009 incidents in which hackers gained administrative control of Twitter due to "serious lapses" in Twitter's data security. One breach in January 2009 resulted in then-President-elect Barack Obama's account getting hacked – a tweet was sent from his account offering his followers a chance to win \$500 in free gasoline. Administrative control of Twitter was achieved through the use of an automated password-guessing tool, which submitted thousands of guesses into Twitter's login webpage. The password was a weak, lowercase, common dictionary word, and no mechanism was in place to suspend or disable an account after a reasonable number of unsuccessful login attempts. During a separate breach in April 2009, a hacker guessed the administrative password of a Twitter employee after compromising the employee's personal email account, where two similar passwords were stored in plain text.

Under the settlement terms agreed to by Twitter, Twitter must establish and maintain a comprehensive security program which will be assessed by an independent auditor every other year for 10 years. It is also barred for 20 years "from misleading consumers about the extent to which it protects the security, privacy, and confidentiality of nonpublic consumer information, including the measures it takes to prevent unauthorized access to nonpublic information and honor the privacy choices made by consumers."

INTERNATIONAL PRIVACY LAWS

- After receiving unanimous approval by the Mexican Congress, Mexico's government

introduced its "Federal Data Protection Law" earlier this month, expanding its oversight power over the collection, processing, and disclosure of personal data from government entities to include the private sector. With the change, Mexico's Federal Institute of Access to Personal Information changed its name to the "Federal Institute of Access to Information and Data Protection." Mexico becomes the latest country to establish a national data protection law administered by a centralized agency, joining the likes of the European Union, Canada, Japan, Hong Kong, New Zealand, Australia, Argentina, Chile, and Paraguay. However, the new Mexican national law does not preempt existing regulatory authorities from issuing privacy regulations. In fact, under Mexico's new dual institutional arrangement, when a data controller breaches its data protection obligations, the issue will first be addressed by the existing regulatory authorities, which are divided by industry, similar to the United States, which continues to maintain a sectoral system of privacy regulation.

August 2010