



ZAG/S&W LLP PRIVACY & DATA SECURITY CLIENT ADVISORY

Privacy & Data Security Law Developments: 2009 Roundup and 2010 Forecast

The fourth quarter of 2009 saw numerous legal developments involving privacy and data security issues, and a number of new regulatory initiatives are pending as we enter 2010. Following is a sampling of news items of particular interest, in each of the five subject matter areas covered by the multi-disciplinary team that comprises Sullivan & Worcester LLP's Privacy & Data Security practice group.

PRIVACY OF CONSUMER INFORMATION AND COMPLIANT MARKETING PRACTICES

- The U.S. House of Representatives on December 8, 2009 approved the "[Data Accountability and Trust Act](#)," HR 2221, which is now pending in the Senate Commerce Committee. This legislation would empower the Federal Trade Commission (FTC) to explicitly regulate data brokers who obtain information about individuals from various sources, then sell or apply analytics to the information to develop consumer profiles for marketing or other purposes. The bill imposes data security, breach notification, and similar obligations on companies that collect and compile data on consumers and also on the companies that use such data. The bill would preempt conflicting state data security laws, but allow state attorneys general to enforce the federal law. Consumers would be empowered to access and correct data compiled about them, much as they can now do with credit reports. The bill also makes it unlawful to collect data under false pretenses.
- A bill introduced in the Senate by Judiciary Committee chair Senator Patrick Leahy of Vermont, [S. 1490](#), also would regulate data brokers, provide consumers access to their records, and require breach notification, and would impose criminal penalties for willfully concealing a data breach. In addition, the bill addresses government use of commercial data and auditing and oversight of data brokers. The bill was reported out of Committee and placed on the Senate legislative calendar on November 5, 2009.
- The FTC signaled its concern about these issues by hosting in December the first of a series of three public roundtable discussions to explore the privacy challenges posed by technology and business practices that collect and use consumer data. This first roundtable focused on the benefits and risks of information-sharing practices, consumer expectations regarding such practices, behavioral advertising, information brokers, and the adequacy of

IF YOU WOULD LIKE ADDITIONAL INFORMATION, PLEASE CONTACT:

Wendy M. Creeden
202 370 3929
wcreeden@zag-sw.com

L. Elise Dieterich
202 370 3925
edieterich@zag-sw.com

David A. Guadagnoli
617 338 2938
dguadagnoli@zag-sw.com

Kimberly B. Herman
617 338 2943
kherman@zag-sw.com

Ilene Robinson Sunshine
617 338 2928
isunshine@zag-sw.com

Kathy L. Cooper
202 370 3926
kcooper@zag-sw.com

Amy K. Lyster
617 338 2804
alyster@zag-sw.com

Christopher T. Stevenson
617 338 2428
cstevenson@zag-sw.com

Ronald P. Whitworth
202 775 1219
rwhitworth@zag-sw.com

BOSTON
ZAG/S&W LLP
One Post Office Square
Boston, MA 02109

NEW YORK
ZAG/S&W LLP
1290 Avenue of the Americas
New York, NY 10104

WASHINGTON, DC
ZAG/S&W LLP
1666 K Street, NW
Washington, DC 20006

ISRAEL
Zysman, Aharoni, Gayer &
Ady Kaplan & Co. / S&W LLP
41-45 Rothschild Blvd., Beit Zion
Tel Aviv, 65784 Israel

existing legal and self-regulatory frameworks. The second roundtable will be held January 28, 2010, in Berkeley, California. See: <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>

- Cloud computing and privacy issues related to data sharing over the Internet also are under scrutiny by the FTC. In comments filed December 9, 2009, in the Federal Communications Commission's National Broadband Plan docket, the FTC stated that "Currently, the FTC is considering cloud computing and identity management as part of a broader initiative to reexamine various models to promote consumer privacy."
- Many companies assume that personal information they have collected from consumers can safely be used, shared or released publicly, provided individual customers' names and other obvious identifying information are removed. Not so according to a class action lawsuit filed against Netflix by a lesbian mother (and others) in a California federal court on December 17, 2009, seeking damages on behalf of all Netflix customers who rented and rated movies on the Netflix Web site from October 1998 through December 2005.

The suit, *Doe v. Netflix*, asserts that a \$1 million contest to improve the Netflix film recommendation system, which ran from 2006 until 2009, disclosed insufficiently anonymized information about its customers in violation of the Video Privacy Protection Act, fair trade laws, and Netflix's own privacy policy. Plaintiff Jane Doe claims that the data released to contest participants risked revealing her sexual orientation, which would "negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's ability to live peaceful lives." Her claim is backed up by research conducted by two University of Texas researchers who claimed they were able to identify several Netflix users by comparing their "anonymous" reviews in the Netflix data to ones posted on the Internet Movie Database Web site. Information the scholars purported to unearth included identifying the reviewers' political leanings and sexual orientation. The suit raises issues similar to those raised in the class action litigation that resulted when AOL released supposedly "anonymized" search-engine logs, which reporters quickly used to track down real people.

PRIVACY OF HEALTHCARE INFORMATION

- In a recent incident that illustrates the dangers both of violating patient confidentiality and of discussing one's work on Twitter, Jennifer Carter, a former Administrative Assistant at University Medical Center (UMC) in Jackson, Mississippi was strongly encouraged to resign (and did so) after a Tweet sent to Governor Haley Barbour referred to a checkup the Governor scheduled at UMC several years ago. After the Governor Tweeted, "Glad the Legislature recognizes our dire fiscal situation. Look forward to hearing their ideas on how to trim expenses," Carter responded, "Schedule medical exams like everyone else instead of paying UMC employees overtime to do it when clinics are usually closed." Governor Barbour's office contacted UMC, whose Compliance Department concluded that Carter's Tweet violated the HIPAA law. Despite Carter's contention that she wasn't "jabbing" at Barbour, and "that's just what people do on Twitter," it resulted in the loss of her job and serves as a stern reminder of the importance of safeguarding all medical information. TV station WLBT's report on the incident is available [here](#).
- A breach of patient records cost Kaiser Permanente more than \$400,000 in fines in 2009, after state regulators in California determined that Kaiser Permanente's Bellflower Hospital failed in two separate incidents to prevent unauthorized access to confidential patient information on octuplets born at the Los Angeles hospital in January. Both incidents relate to patient records associated with Nadya Suleman's birth of eight babies in the hospital on Jan. 26, which were found to have been improperly viewed by eight Kaiser employees, two doctors, and 21 other patients.
- Celebrity records, however, are not the only medical records at risk. For example, on November 18, 2009, Connecticut Attorney General Richard Blumenthal announced that his office would investigate health benefit provider Health Net for the loss of nearly 450,000 Connecticut residents' health, personal and financial information, coupled with a six-month delay in informing consumers and the state of the breach, both possible violations of state and federal law. Blumenthal expressed outrage at Health Net's delay in informing consumers and regulators of the loss, "leaving [the consumers] naked to identity theft," among other concerns.

- The HITECH amendments to the HIPAA law included in the 2009 American Recovery and Reinvestment Act (the so-called Stimulus Bill) impose heightened obligations on companies (“business associates”) that handle patient records in connection with providing services to the healthcare industry. Also, pursuant to HITECH, both the FTC and the U.S. Department of Health and Human Services (HHS) in 2009 issued new health data breach notification rules, and are considering the unique privacy and data security implications of electronic medical records, particularly when shared among entities or stored in a cloud computing environment. HHS reportedly has announced plans to hire a contractor to test whether “anonymized” data in fact protects the privacy of individual health records – a key issue as the drive to use healthcare IT and electronic health records for research and marketing purposes increases.

PRIVACY OF FINANCIAL INFORMATION

- On November 17, 2009, eight federal regulatory agencies released a final model privacy notice form for the financial industry developed through extensive research and testing, designed to make it easier for consumers to understand how financial institutions collect and share consumer information. A 2006 amendment to the Gramm-Leach-Bliley Act (GLBA) required the agencies to propose a succinct and comprehensible model form with an easy-to-read font, allowing consumers to easily compare the privacy practices of different financial institutions. Under the GLBA, institutions must notify consumers of their information-sharing practices and their right to opt out of certain sharing practices. The model form can be used by financial institutions to comply with those requirements. The agencies released [one version](#) offering an opt-out provision, and [another](#) without.
- The FTC has continued to experience resistance to full implementation of its “Red Flags Rule” designed to help prevent identity theft, which became law in 2008. In a press release issued on October 30, 2009, the FTC announced its fourth delay in the enforcement of the Rule until June 1, 2010, in response to a request from several members of Congress. The request came just two days prior to the expiration of the FTC’s latest enforcement postponement, and nine days following the House of Representatives’ unanimous approval of a bill enacting significant Rule exemptions. The further delay was requested to allow Congress to finalize legislation. See <http://www.sandw.com/news-publications-261.html>

WORKPLACE PRIVACY

- The U.S. Supreme Court announced on December 14, 2009 that it will hear a case that could have a profound effect on employees’ privacy expectation rights when using employer-provided equipment. In [City of Ontario v. Quon](#), the Ninth Circuit upheld the Ontario (CA) Police Department’s policy allowing it to monitor text messages sent on Department-issued devices. The question arose when transcripts of a police sergeant’s text messages were accessed by a lieutenant (despite prior, informal reassurances that they would not be inspected), and the transcript revealed sexually-explicit messages.
- Employee records received heightened privacy protections under 2009 regulations promulgated in Massachusetts, which implemented controversial data protection rules applicable to any natural person, corporation, association, partnership or other legal entity that owns, licenses, stores, or maintains certain “personal information” about a resident of Massachusetts. This includes any business that employs Massachusetts residents, if its employee records include certain personal information. For purposes of the new rules, “personal information” is defined as a Massachusetts resident’s first name and last name, or first initial and last name, combined with one or more of: (i) a Social Security number, (ii) a drivers license or state-issued identification number, or (iii) a financial account or debit or credit card number. The regulations impose numerous data security requirements including the obligation, when a business no longer requires a resident’s personal information, to permanently destroy any records containing that information.

In response to objections from businesses that the rules are proving to be excessively burdensome and costly to implement, it was announced in August that enforcement of the rules is being postponed until March 1, 2010, and that certain provisions of the regulations would be modified to ease compliance. See <http://www.sandw.com/news-publications-248.html>

BREACH MANAGEMENT AND LITIGATION

- Along with Netflix and Kaiser Permanente, discussed above, numerous other companies experienced in 2009 the financial and public relations damages that an unauthorized release of protected data can cause. CFO Magazine reported:

“Security attacks are not lessening with the economic downturn; in fact, research shows

just the opposite. The number of data breaches at businesses, government agencies, and educational institutions in the United States jumped by nearly 50 percent in 2008 compared with 2007, according to the Identity Theft Resource Center (ITRC), a nonprofit organization that supports victims of identity theft and broadens public awareness of the problem.

The ITRC says there were 656 breaches reported in 2008 — up 47 percent from the year before — exposing more than 35 million electronic records. (This data doesn't reflect the Heartland incident, which took place in 2008 but was announced [in 2009] and had yet to be adequately assessed as of press time.) The breaches took many forms and were perpetrated by both outsiders and insiders, but many shared a common trait: they were easy to pull off. A mere 2.4 percent of all breaches required the perpetrators to foil encryption or other strong protection methods; password protection was in place in fewer than 10 percent of the cases."

- Heartland Payment Systems, a New Jersey-based payment processor, continues to realize the monetary costs of its massive 2008 data breach, as it announced a \$3.6 million settlement with American Express on December 17, 2009. The New Jersey-based payments processor was victimized by hackers, which accessed its system to steal more than 130 million credit card numbers. Heartland reportedly lost \$500 million in stock value (3/4ths of its market capitalization) and has spent more than \$32 million in legal fees, fines, settlements and forensics. Sixteen class action complaints by financial institutions were filed against it. On December 21, 2009, Heartland announced that it also was settling the consumer cardholder class actions consolidated in the United States District Court for the Southern District of Texas. Under the terms of the settlement, Heartland will pay a minimum of \$1,000,000 and up to a maximum of \$2,400,000 to class members who submit valid claims for losses as a result of the intrusion. Heartland also will pay all costs associated with the administration of the settlement, including up to \$1.5 million for the cost of notice to the settling class, and will pay up to \$760,000 of the plaintiffs' attorneys' fees and costs.

* * *

For more information on these matters, and answers to questions regarding privacy and data security issues, please [contact us](#). We look forward to being of service.

January 2010