

CLIENT ALERT

HUNTON & WILLIAMS

April 2010

This Client Alert is a monthly update on privacy and information management developments as posted on Hunton & Williams' [Privacy and Information Security Law Blog](#). If you would like to receive email alerts when new posts are published, please visit our [blog](#) and enter your email address in the subscribe field.

Recent posts on the Privacy and Information Security Law blog include:

- [Department of Commerce to Seek Public Comment on Privacy Issues](#)
- [International Data Protection Authorities Scold Google Over Privacy Concerns](#)
- [Mexico on the Verge of Amending its Data Protection Law](#)
- [Italian Court's Reasoning in Google Case Released](#)
- [FINRA Fines Montana Brokerage Firm \\$375,000 for Failure to Protect Customer Information](#)
- [New Zealand Privacy Commissioner Discusses Global Standards](#)
- [Mississippi Becomes 46th State to Enact Breach Notification Law](#)
- [Behavioral Advertising Complaint Filed with the FTC](#)
- [New Jersey Supreme Court's Ruling Advances Employee Privacy](#)
- [Attorney General Launches New HIPAA Investigation](#)
- [Addition to Washington Breach Law Imposes Retailer Liability in Payment Card Breaches](#)
- [FTC's Revised Free Credit Reports Rule Becomes Effective April 2, 2010](#)

Department of Commerce to Seek Public Comment on Privacy Issues

April 22, 2010

On April 20, 2010, the Department of Commerce ("DOC") issued a [Notice of Inquiry](#) to solicit public feedback "on the impact of current privacy laws in the United States and around the world on the pace of innovation in the information economy." The aim is to understand "whether current privacy laws serve consumer interests and fundamental democratic values." To this end, the DOC poses a number of questions. [Continue Reading...](#)

International Data Protection Authorities Scold Google Over Privacy Concerns

April 21, 2010

On April 19, 2010, the Privacy Commissioner of Canada, Jennifer Stoddart, and the heads of nine other international data protection authorities took part in an unprecedented collaboration by issuing a [strongly worded letter](#) of reproach to Google's Chief Executive Officer, Eric Schmidt. The joint letter, which was also signed by data protection officials from France, Germany, Ireland, Israel, Italy, the Netherlands, New Zealand, Spain and the United Kingdom, highlighted growing international concern that "the privacy rights of the world's citizens are being forgotten as Google rolls out new technological applications." [Continue Reading...](#)

Mexico on the Verge of Amending its Data Protection Law
April 14, 2010

According to Mr. M. Jorge Yanez V., a partner at the law firm of Barrera, Siqueiros y Torres Landa, S.C. in Mexico City, on April 13, 2010, the House of Representatives of Mexico passed a bill that, when ratified by the Senate, will become the country's new Federal Law of Protection of Personal Information. The Senate is expected to pass the bill shortly and without revisions. When the bill is enacted into law, Mexico's Federal Institute of Access to Information, the agency that currently oversees the disclosure of and access to government information, will be renamed the Federal Institute of Access to Information and Data Protection. The agency's jurisdiction will expand to include the protection of personal information of private individuals and entities. We will provide additional details about the new bill as it becomes available.

Italian Court's Reasoning in Google Case Released
April 14, 2010

Following up on our [previous post on the sentencing of three Google executives](#) by an Italian court, the [New York Times reports](#) that an 111-page explanation of the verdict has been released. Judge Oscar Magi found that Google had an obligation to make users more aware of its EU privacy policies, and cited Google's active marketing of its Google Video site as indicative of the company's profit motive for not removing the video sooner.

FINRA Fines Montana Brokerage Firm \$375,000 for Failure to Protect Customer Information
April 13, 2010

On April 12, 2010, the Financial Industry Regulatory Authority ("FINRA") [announced that it had fined D.A. Davidson & Co. \\$375,000](#) for failing to protect its customers' confidential information. In late 2007, the firm's system was compromised when hackers employed a SQL injection attack to download the confidential customer information of approximately 192,000 individuals. The security breach came to light when one of the persons responsible for the intrusion attempted to blackmail D.A. Davidson via email on January 16, 2008. The firm responded quickly by notifying law enforcement authorities and providing affected individuals with two years of credit monitoring. While D.A. Davidson neither admitted nor denied the charges in settling the case, the firm consented to the entry of FINRA's findings. To date, there has been no evidence of identity theft resulting from this incident.

New Zealand Privacy Commissioner Discusses Global Standards
April 13, 2010

In a decision handed down on February 25, 2010, the French Constitutional Court ruled that the right to privacy derives from Article 2 of the [Declaration of Human Rights](#), and is therefore considered a constitutional right under French law. The Court also ruled that the legislature must strike a balance between the right to privacy and other fundamental interests, such as preventing threats to public safety, which are necessary to preserve constitutional rights and principles. [Continue Reading...](#)

Mississippi Becomes 46th State to Enact Breach Notification Law
April 9, 2010

On April 7, 2010, Mississippi became the 46th state to enact a [data security breach notification law](#). The law, which will take effect July 1, 2011, applies to the unauthorized acquisition of unencrypted electronic files, media, databases or computerized data containing personal information of any Mississippi resident. The law contains a harm threshold specifying that notification is not required if it can be reasonably determined that the breach will not likely result in harm to affected individuals. The enactment of this law

leaves Alabama, Kentucky, New Mexico and South Dakota as the only remaining states without a legal requirement to notify affected individuals in the event of a breach.

Our last [update on state breach notification laws](#) was in August, 2009, when we reported on Missouri's enactment of a similar statute.

Behavioral Advertising Complaint Filed with the FTC

April 8, 2010

Today three advocacy organizations filed a [complaint](#) with the Federal Trade Commission ("FTC"), demanding that it investigate and impose drastic requirements on entities involved in online data analytics and behavioral advertising. In their complaint, the U.S. Public Interest Research Group ("U.S. PIRG"), the Center for Digital Democracy and the World Privacy Forum target Google, Yahoo!, BlueKai, PubMatic, TARGUSinfo and others for allegedly participating in what the U.S. PIRG terms a "[Wild West](#)" of online collection and auctioning of data for marketing purposes. [Continue Reading...](#)

New Jersey Supreme Court's Ruling Advances Employee Privacy

April 2, 2010

On March 30, 2010, the New Jersey Supreme Court ruled for the former employee in *Stengart v. Loving Care Agency, Inc.* on the employee's claim that state common privacy law protected certain of her emails from review by the employer. [Continue Reading...](#)

Attorney General Launches New HIPAA Investigation

April 1, 2010

The Attorney General of Connecticut, Richard Blumenthal, is investigating an alleged breach of medical records at Griffin Hospital in Derby, Connecticut. The hospital believes that a formerly affiliated radiologist gained unauthorized access to its digital Picture Archiving and Communications System ("PACS"), which stores patient information, including names, exam descriptions and medical record numbers. In February, the hospital began receiving inquiries from patients who had been contacted by the radiologist to promote professional services offered at another medical facility. In response to patient inquiries, the hospital conducted an internal investigation that revealed several instances of unauthorized access to the PACS system. The hospital subsequently notified Attorney General Blumenthal. [Continue Reading...](#)

Addition to Washington Breach Law Imposes Retailer Liability in Payment Card Breaches

March 24, 2010

Under a Washington law effective July 1, 2010, certain entities involved in payment card transactions may be liable to financial institutions for costs associated with reissuing payment cards after security breaches. Designed to encourage the reissuance of payment cards as a means of mitigating harm caused by security breaches, [Washington H.B. 1149](#) applies to three types of entities: *businesses*, *processors* and *vendors*. Under the law, a *business* is an entity that "processes more than six million credit card and debit card transactions annually, and who provides, offers, or sells goods or services to . . . residents of Washington." A *processor* is any entity, other than a *business*, that "directly processes or transmits [payment card] account information for or on behalf of another person as part of a payment processing service." A *vendor* is any "entity that manufactures and sells software or equipment that is designed to process, transmit, or store [payment card] account information or that maintains account information that it does not own." [Continue Reading...](#)

FTC's Revised Free Credit Reports Rule Becomes Effective April 2, 2010
March 24, 2010

Provisions of the FTC's revised rule that regulate advertisements for free credit reports become effective April 2, 2010. As required by the Credit CARD Act of 2009, the FTC promulgated the revised rule on February 22, 2010, to prevent the deceptive marketing of free credit reports by companies that required consumers to sign up for paid products and services such as credit monitoring in order to receive the reports. [Continue Reading...](#)



Visit the Privacy and Information Security Law Blog at www.huntonprivacyblog for global privacy and information security law updates and analysis.