CLIENT ALERT

HUNTON& WILLIAMS

December 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:

- President Obama Signs Red Flag Program Clarification Act
- Court Finds Fourth Amendment Protects Email Privacy
- German DPAs Set Minimum Qualification and Independence Requirements for Company Data Protection Officers
- Department of Commerce Issues Landmark Privacy Green Paper
- Senator Kerry's Senior Advisor Provides Key Insight into Forthcoming Privacy Bill
- House Approves Social Security Number Protection Act
- French Data Protection Authority Revises Authorization on Whistleblowing Schemes
- House Hears Testimony on Do Not Track Legislation
- European Parliament Hosts Privacy Platform on Comprehensive Data Protection Framework
- FTC Issues Landmark Privacy Report
- Vladeck Previews Long-Awaited FTC Report
- Wake Up Call for UK Data Controllers: ICO Issues its First Fines for Data Breaches
- Dutch Bill Proposes Data Breach Notification Requirements and Revised Cookie Regime

---

President Obama Signs Red Flag Program Clarification Act

December 20, 2010

On December 18, 2010, President Obama signed into law the "Red Flag Program Clarification Act of 2010" (S.3987), which amends the Fair Credit Reporting Act with respect to the applicability of identity theft guidelines to creditors. The law limits the scope of the Federal Trade Commission's Identity Theft Red Flags Rule ("Red Flags Rule"), which requires "creditors" and "financial institutions" that have "covered accounts" to develop and implement written identity theft prevention programs to help identify, detect and respond to patterns, practices or specific activities that indicate possible identity theft. Continue Reading…

Court Finds Fourth Amendment Protects Email Privacy

December 17, 2010

On December 14, 2010, the United States Court of Appeals for the Sixth Circuit ruled in *United States v. Warshak* that a "subscriber enjoys a reasonable expectation of privacy in the content of emails" stored, sent or received through a commercial internet service provider ("ISP"). According to the court, the government must have a search warrant before it can compel a commercial ISP to turn over the contents of a subscriber's emails.

In 2008, a jury sitting in the Southern District of Ohio convicted defendants Steven Warshak, Harriet Warshak and TCI Media, Inc. of various crimes relating to defrauding customers of Berkeley Premium Nutraceuticals, Inc. Before trial, Warshak's motion to exclude thousands of emails that the government

obtained from his ISP was denied. The defendants appealed their convictions, arguing that the government's warrantless seizure of Warshak's private emails violated the Fourth Amendment's prohibition on unreasonable searches and seizures. Continue Reading…

German DPAs Set Minimum Qualification and Independence Requirements for Company Data Protection Officers

December 17, 2010

On November 25, 2010, the German data protection authorities responsible for the private sector (also known as the "Düsseldorfer Kreis") issued a resolution on the minimum requirements for the qualifications and independence of company data protection officers ("DPOs"). This initiative follows inspections carried out within companies that revealed a generally insufficient level of expertise among DPOs given data processing complexities and the requirements set by the Federal Data Protection Act. The DPAs recognize that a DPO's workload depends primarily on the size and number of data controllers the DPO supervises, industry-specific factors related to data processing and the level of protection required for the types of personal data being processed. Changes with respect to these factors frequently increase the burden on DPOs without a compensating increase in resources needed to ensure proper oversight. Continue Reading…

Department of Commerce Issues Landmark Privacy Green Paper

December 16, 2010

On December 16, 2010, the U.S. Department of Commerce Internet Policy Task Force issued its "Green Paper" on privacy, entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." The Green Paper outlines Commerce's privacy recommendations and proposed initiatives, which contemplate the establishment of enforceable codes of conduct, collaboration among privacy stakeholders, and the creation of a Privacy Policy Office in the Department of Commerce. Noting that "privacy protections are crucial to maintaining the consumer trust that nurtures the Internet's growth," the Green Paper "recommends reinvigorating the commitment to providing consumers with effective transparency into data practices, and outlines a process for translating transparency into consumer choices through a voluntary, multistakeholder process." Continue Reading…

Senator Kerry's Senior Advisor Provides Key Insight into Forthcoming Privacy Bill

December 10, 2010

On December 10, 2010, Senior Advisor to U.S. Senator John Kerry (D-Mass.), Daniel Sepulveda, briefed the Centre for Information Policy Leadership at Hunton & Williams LLP (the "Centre") members on Senator Kerry's forthcoming privacy legislation. The bill, which will be introduced next Congress, aims to establish a regulatory framework for the comprehensive protection of individuals' personal data that authorizes rulemakings by the Federal Trade Commission. Continue Reading…

House Approves Social Security Number Protection Act

December 9, 2010

On December 8, 2010, the U.S. House of Representatives approved the Social Security Number Protection Act of 2010 (S. 3789), which is aimed at reducing identity theft by limiting access to Social Security numbers. The bill prohibits printing Social Security numbers, or any derivative of a Social Security number, on government-issued checks, and bars federal, state and local government entities from employing prisoners in jobs that would allow them to access Social Security numbers. Although there are numerous state laws on the books to safeguard Social Security numbers, the Social Security Number Protection Act will provide federal coverage. The bill was introduced by Senators Dianne

Feinstein (D-CA) and Judd Gregg (R-NH) and passed in the Senate by unanimous consent on September 28, 2010. It is now headed for signature by President Obama.

French Data Protection Authority Revises Authorization on Whistleblowing Schemes
December 8, 2010

On October 14, 2010, the French Data Protection Authority (the "CNIL") adopted several amendments to its single authorization AU-004 regarding the use of whistleblowing schemes (the "Single Authorization").

Since 2005, companies in France must register their whistleblowing schemes with the CNIL either by self-certifying to the CNIL's Single Authorization or by filing a formal request for approval with the CNIL. Companies that self-certify to the Single Authorization make a formal undertaking that their whistleblowing scheme complies with the pre-established conditions set out in this authorization. In particular, the scope of the Single Authorization is limited to the following specific areas: finance, accounting, banking, fight against corruption and compliance with Section 301(4) of the Sarbanes-Oxley Act. Under the revised framework, the CNIL has extended the scope of the Single Authorization to include the prevention of anti-competitive practices and compliance with the Japanese Financial Instrument and Exchange Act. Continue Reading…

House Hears Testimony on Do Not Track Legislation
December 3, 2010

On December 2, 2010, discussions about privacy continued at a hearing on "Do Not Track Legislation: Is Now the Right Time?" held by the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection. The hearing focused on a variety of consumer privacy issues, including the implications and challenges of a Do Not Track mechanism, the consumer's desire for more control over the collection and use of their data and tracking practices, and the need to preserve an advertising supported Internet that promotes economic growth through online business. Continue Reading…

European Parliament Hosts Privacy Platform on Comprehensive Data Protection Framework
December 2, 2010

On December 1, 2010, the European Parliament hosted a Privacy Platform on the European Commission's recent Communication proposing "a comprehensive approach on personal data protection in the European Union," which is aimed at modernizing the current EU data protection framework. The panel, hosted by European Parliament Member Sophie in 't Veld, included:

- The Head of Cabinet of the European Commission's Commissioner for Justice, Fundamental Rights and Citizenship, Martin Selmayr (in Commissioner Viviane Reding's absence);
- The Chairman of the Article 29 Working Party, Jacob Kohnstamm; and
- The European Data Protection Supervisor, Peter Hustinx.

The Platform was very well attended, bringing together a wide range of stakeholders from both the public and private sectors. Continue Reading…

FTC Issues Landmark Privacy Report
December 1, 2010

On December 1, 2010, the Federal Trade Commission released its long-awaited report on online privacy entitled "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers." Observers expected the report to address the concept of privacy by design, the burdens placed on consumers to read and understand privacy notices and make privacy choices, the provision of individual access to personal data and the rights of consumers with respect to Internet tracking. The FTC report introduces a privacy framework to "establish certain common assumptions and bedrock protections on which both consumers and businesses can rely as they engage in commerce." It includes the following elements: Continue Reading…

Vladeck Previews Long-Awaited FTC Report
December 1, 2010

David Vladeck, Director of the FTC's Division of Consumer Protection, this morning previewed the long-awaited FTC report that sums up months of discussion regarding the future of privacy regulation in the United States and examines the viability of a Do Not Track mechanism. Vladeck indicated at the Consumer Watchdog Policy Conference that the existing privacy framework in the U.S. is not keeping pace with new technologies. In addition, he stated that the pace of industry self-regulation, while constructive, has been too slow. According to Vladeck, the report will address several major themes, including the following: Continue Reading…

Wake Up Call for UK Data Controllers: ICO Issues its First Fines for Data Breaches
November 25, 2010

In the first use of his powers to impose monetary penalties, the UK Information Commissioner has announced fines for two organizations with respect to serious breaches of the UK Data Protection Act.

- Hertfordshire County Council must pay a fine of £100,000 after staff accidentally faxed highly sensitive information to the wrong recipients, on two separate occasions.
- A4e Limited, an employment services company, must pay £60,000 following the theft of an unencrypted laptop from an employee's home, putting the data of 24,000 people at risk.

Continue Reading…

Dutch Bill Proposes Data Breach Notification Requirements and Revised Cookie Regime
November 16, 2010

In a move toward implementation of the EU e-Privacy Directive, on November 3, 2010, the Dutch Minister of Economic Affairs submitted a bill to the Dutch Parliament that would amend the Dutch Telecommunications Act to obligate telecom and internet service providers to provide notification of data security breaches, and require consent for the use of cookies (the "Bill").

The proposed Bill would require telecom and internet service providers to notify the Dutch Telecom Authority (the "OPTA") without delay in the event of a security breach involving personal data. They also would be required to notify affected individuals without delay if the breach is likely to have an adverse effect on the protection of their personal data. The Bill does not affect initiatives to introduce a broader data breach notification regime applicable to other industries outside the telecom sector. The Dutch Minister of Justice recently stated that he expects to issue a proposal to implement a more general data breach notification law in 2011. Continue Reading…

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