CLIENT ALERT

HUNTON& WILLIAMS

April 2011

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:

Another Sony Service Breached by Hackers
May 3, 2011

On May 2, 2011, Sony Computer Entertainment America ("Sony") disclosed that hackers had gained access to the personal information of 24.6 million customers who played games on the Sony Online Entertainment ("SOE") network. Sony stated that hackers may have accessed names, addresses and birth dates of SOE gaming customers, as well as credit card data of about 12,700 non-U.S. accounts and 10,700 bank account numbers from "an outdated database from 2007." Sony clarified that the SOE breach was not the result of a second attack, but rather occurred as part of the broad incursion against the company that affected 77 million PlayStation accounts, as the company previously disclosed on April 26. Continue Reading…

Authorities in Austria and Switzerland Rule on Google Street View
May 3, 2011

Austrian DPA Gives Green Light Subject to Conditions

On April 21, 2011, the Austrian Data Protection Commission ("Austrian DPA") published its decision allowing Google to register its Google Street View application on the Austrian DPA's data processing register. As part of the registration procedure, Google agreed to blur images of faces and license plates prior to publishing them on the Internet, and to provide information to the public about the right to object to publication of certain images. Continue Reading…

French Data Protection Authority Unveils its Goals for 2011 Inspections
April 27, 2011

On April 26, 2011, the French Data Protection Authority (the "CNIL") issued a press release unveiling its inspection goals for the coming year. In a report adopted on March 24, 2011, the CNIL indicated that it intends to conduct at least 400 inspections in France (100 more than the 2010 goal), with a special focus on the following issues: Continue Reading…

Europe's Online Advertising Industry Agrees on Self-Regulatory Framework
April 22, 2011

On April 14, 2011, the European Advertising Standards Alliance ("EASA") and IAB Europe released complementary new self-regulatory standards for online behavioral advertising. This cross-industry initiative is aimed at enhancing European consumers' control over their data and ensuring transparency, particularly with respect to advertisements that are delivered using third party online behavioral advertising. Continue Reading…

Court Finds Allegations of Harm Sufficient to Allow Breach-Related Class Action Suit to Proceed
April 22, 2011

On April 11, 2011, the United States District Court for the Northern District of California declined to dismiss four of the nine claims in a class action lawsuit filed against RockYou, Inc. ("RockYou"), a publisher and developer of applications used on popular social media sites. The suit stems from a December 2009 security breach caused by an SQL injection flaw that resulted in the exposure of unencrypted user names and passwords of approximately 32 million RockYou users. RockYou subsequently fixed the error and acknowledged in a public statement that "one or more individuals had illegally breached its databases" and that "at the time of the breach, the hacked database had not been up to date with industry standard security protocols." After receiving notification of the security breach from RockYou in mid-December, on December 28, 2009, a RockYou user who had signed up for a photo-sharing application filed a complaint seeking injunctive relief and damages for himself and on behalf of all other similarly-situated individuals. Continue Reading…

European Commission Presents Evaluation Report on Telecommunications Data Retention
April 19, 2011

On April 18, 2011, the European Commission (the "Commission") adopted an Evaluation Report on the EU Data Retention Directive 2006/24/EC (the "Data Retention Directive").

The Data Retention Directive requires that, for law enforcement purposes, telecommunications service and network providers ("Operators") must retain certain categories of telecommunications data (excluding the content of the communication) for not less than six months and not more than two years. To date, most of the EU Member States have implemented the Data Retention Directive, but Czech Republic, Germany and Romania no longer have implementing laws in place because their constitutional courts have annulled the implementing laws as unconstitutional. Continue Reading…

Article 29 Working Party Releases Opinion on Smart Metering
April 18, 2011

On April 4, 2011, the Article 29 Working Party (the "Working Party") issued an Opinion to clarify the legal framework applicable to smart metering technology in the energy sector (the "Opinion"). Smart meters are digital meters that record energy consumption and enable two-way remote communication with the wider network for purposes such as monitoring and billing, and to forecast energy demand. Smart meters are intended to allow the industry to better regulate energy supply, and to help individuals reduce consumption. According to the Working Party, however, the analysis and exchange of smart metering information has the potential to be privacy-invasive. Continue Reading…

UK Government Announces Implementation of EU Cookies Law
April 18, 2011

On April 15, 2011, the United Kingdom's Department for Culture, Media and Sport ("DCMS") announced that the UK will adopt the new EU rules on cookies without "gold-plating" the regulations by imposing additional national requirements, to help ensure that British companies can compete with the rest of Europe. As we previously reported, the UK government had reassured businesses that it would carry out the implementation in a manner that would minimize the impact on businesses and consumers. Continue Reading…

Representative Stearns Introduces Consumer Privacy Protection Act
April 15, 2011

On April 13, 2011, Representative Cliff Stearns (R-FL) introduced the Consumer Privacy Protection Act of 2011 (the "Act"), which seeks to "protect and enhance consumer privacy" both online and offline by imposing certain notice and choice requirements with respect to the collection and use of personal information. Continue Reading…

Article 29 Working Party Finds New Zealand's Data Protection Regime Adequate
April 13, 2011

On April 4, 2011, the Article 29 Working Party (the "Working Party") issued an Opinion finding that New Zealand ensures an adequate level of data protection within the meaning of the EU Data Protection Directive 95/46/EC (the "Data Protection Directive"). The Working Party's assessment in the Opinion focuses on the New Zealand Privacy Act 1993 and is based primarily on a comparison of the Act and relevant case law, against the provisions of the Data Protection Directive. Continue Reading…

Senators Kerry and McCain Introduce the Commercial Privacy Bill of Rights Act of 2011
April 12, 2011

On April 12, 2011, U.S. Senators John Kerry (D-MA) and John McCain (R-AZ) introduced the Commercial Privacy Bill of Rights Act of 2011 (the "Act") to "establish a regulatory framework for the comprehensive protection of personal data for individuals under the aegis of the Federal Trade Commission." The bill applies broadly to entities that collect, use, transfer or store the "covered information" of more than 5,000 individuals over a consecutive 12-month period. Certain provisions of the bill would direct the FTC to initiate rulemaking proceedings within specified timeframes, but the bill also imposes requirements directly on covered entities. Continue Reading…

Email Marketing Service Provider's Data Breach Likely to Affect Millions
April 4, 2011

On April 1, 2011, Epsilon Data Management, LLC ("Epsilon"), a leading marketing services provider based in Irving, Texas, issued a press release announcing that its clients' customer data had been "exposed by an unauthorized entry into Epsilon's email system" that took place on March 30, 2011. In the press release, Epsilon indicated that the information acquired as a result of the incident was limited to email addresses and customer names. Several major retailers, credit card issuers, financial institutions and other companies that use Epsilon as a service provider have since notified their customers of the incident. According to the various company statements and emails to customers distributed as a result of this incident, no other personal information (such as bank account information, credit card numbers or Social Security numbers) was compromised. Potentially affected customers are being warned of possible "phishing" attacks that could be linked to the information acquired as a result of this incident. Epsilon's breach has the potential to be one of the largest in U.S. history.

States Attempt to Address Privacy Risks Associated with Digital Copiers and Electronic Waste
April 1, 2011

As reported in *BNA's Privacy Law Watch*, on April 1, 2011, a New York law went in effect requiring manufacturers of certain electronic equipment, including devices that have hard drives capable of storing personal information or other confidential data, to register with the Department of Environmental Conservation and maintain an electronic waste acceptance program. The program must include convenient methods for consumers to return electronic waste to the manufacturer and instructions on how consumers can destroy data on the devices before recycling or disposing of them. Retailers of covered electronic equipment will be required to provide consumers with information at the point of sale about opportunities offered by manufacturers for the return of electronic waste, to the extent they have been provided such information by the manufacturer. Continue Reading…

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