PRIVACY AND INFORMATION SECURITY LAW BLOG
GLOBAL PRIVACY AND INFORMATION SECURITY LAW UPDATES AND ANALYSIS

May 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:

- Complaint to FTC Alleges Cloud Service Dropbox Fails to Sync Security with Representations
- FCRA Claim Against Spokeo Allowed to Proceed
- UK ICO Gives Websites One Year to Comply with New Cookies Law
- Article 29 Working Party Opines on Geolocation Services
- White House Proposes Cybersecurity Legislation
- India Drafts New Privacy Regulations
- California Bill Targets Social Networking Privacy
- German Federal Office for Information Security Issues Final Framework Paper on Information Security for Cloud Computing
- Disney Subsidiary Settles FTC COPPA Violation Charges with $3 Million Penalty
- UK ICO Releases Code on Data Sharing
- Senator Rockefeller Introduces the Do-Not-Track Online Act of 2011
- Supreme Court Hears Oral Argument in Sorrell v. IMS Health
- Ceridian and Lookout Services Settle FTC Charges over Failure to Secure Customers' Personal Information

---

Complaint to FTC Alleges Cloud Service Dropbox Fails to Sync Security with Representations

May 26, 2011

According to a complaint submitted to the Federal Trade Commission on May 11, 2011, the popular cloud-based data storage provider Dropbox, Inc. made false claims about the security of its users' data, thereby putting them at risk while gaining an unfair advantage over competitors that actually offer the sort of security Dropbox advertised. The Dropbox service allows users to create folders on their computers that automatically sync with corresponding folders on Dropbox's servers. Users can specify whether their folders are public or private. The allegations concern the folders designated as private, which are touted as being protected by encryption. According to the complaint, which was filed by Christopher Soghoian (a security researcher and former technologist at the FTC's Division of Privacy and Identity Protection), although Dropbox represented that its encryption features would render a user's files completely inaccessible to any person other than the user, in fact, Dropbox employees maintained copies of the encryption keys and could therefore access the contents of users' files. This left Dropbox users' files susceptible to unauthorized access (e.g., governmental demands for data, hacking attacks, rogue insiders). Continue Reading…

FCRA Claim Against Spokeo Allowed to Proceed
May 26, 2011

On May 11, 2011, in *Thomas Robins v. Spokeo, Inc.*, the United States District Court for the Central District of California granted in part and denied in part defendant Spokeo, Inc.'s motion to dismiss claims that it violated the Fair Credit Reporting Act ("FCRA"). The ruling allows the plaintiff to continue his action against Spokeo, a website that aggregates data about individuals from both online and offline sources. Continue Reading…

UK ICO Gives Websites One Year to Comply with New Cookies Law
May 25, 2011

On May 25, 2011, the UK Information Commissioner's Office (the "ICO") issued a news release stating that organizations and businesses that run websites aimed at UK consumers will be given up to 12 months to "get their house in order" before enforcement of the new cookie law begins. Information Commissioner Christopher Graham made it clear, however, that "[t]his does not let everyone off the hook. Those who choose to do nothing will have their lack of action taken into account when we begin formal enforcement of the rules." Continue Reading…

Article 29 Working Party Opines on Geolocation Services
May 19, 2011

On May 16, 2011, the Article 29 Working Party (the "Working Party") adopted an Opinion on geolocation services on smart mobile devices (the "Opinion"). The Opinion clarifies the legal framework and obligations applicable to geolocation services such as maps and navigation tools, geo-personalized services, geotagging of content on the Internet, child control and location-based advertising. Continue Reading…

White House Proposes Cybersecurity Legislation
May 19, 2011

As we reported last week, on May 12, 2011, the Obama administration announced a comprehensive cybersecurity legislative proposal in a letter to Congress. The proposal, which is the culmination of two years of work by an interagency team made up of representatives from multiple departments and agencies, aims to improve the nation's cybersecurity and protect critical infrastructure. If enacted, this legislation will affect many government and private-sector owners and operators of cyber systems, including all critical infrastructure, such as energy, financial systems, manufacturing, communications and transportation. In addition, the proposal includes a wide-reaching data breach notification law that is intended generally to preempt the existing state breach laws in 46 states plus Washington, D.C., Puerto Rico and the U.S. Virgin Islands. Continue Reading…

India Drafts New Privacy Regulations
May 18, 2011

On April 11, 2011, India adopted new privacy regulations, known as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the "Rules"). The Rules are final versions of the draft regulations issued in February 2011 and impose wide-ranging obligations on any "body corporate" (company) that "collects, receives, possesses, stores, deals or handles" personal information. These obligations require companies to provide privacy policies, restrict the processing of sensitive personal data, restrict international data transfers and require

additional security measures. The Rules introduce an omnibus privacy law that is similar in many respects to existing EU data protection law, but which raises some fundamental challenges for India's numerous outsourcing vendors, and their customers. Continue Reading…

California Bill Targets Social Networking Privacy
May 17, 2011

A new bill proposed in California, the Social Networking Privacy Act (the "Act"), would force social networking websites to establish a default privacy setting for its users that prohibits the site from publicly displaying most information about the user without the user's consent. Many social networking websites currently utilize a default setting where a user's personal information, interests and photos are public until a user changes those settings, so the Act would represent a fundamental shift in social networking privacy. Continue Reading…

German Federal Office for Information Security Issues Final Framework Paper on Information Security for Cloud Computing
May 16, 2011

On May 10, 2011, the German Federal Office for Information Security, (the *Bundesamt für Sicherheit in der Informationstechnik* or "BSI") released the final framework paper on information security issues related to cloud computing. The paper describes the minimum requirements for information security for cloud computing services. As we previously reported, in September 2010, the BSI had presented the draft framework paper which received positive reviews and constructive comments from cloud computing providers, users, associations and other stakeholders. The comments and contributions have been incorporated in the final framework paper. According to the BSI, the paper provides "Best Practices" and serves as a basis for the discussion between cloud computing service providers and cloud users. Based on the paper, concrete recommendations for companies or public authorities may be developed, including at the international level.

Disney Subsidiary Settles FTC COPPA Violation Charges with $3 Million Penalty
May 13, 2011

On May 12, 2011, the Federal Trade Commission announced that Playdom, Inc., a Disney subsidiary, has agreed to pay $3 million to settle charges that the company violated Section 5 of the FTC Act and the Children's Online Privacy Protection Rule ("COPPA Rule") "by illegally collecting and disclosing personal information from hundreds of thousands of children under age 13 without their parents' prior consent." This settlement marks the largest civil penalty imposed for an FTC COPPA Rule violation. Continue Reading…

UK ICO Releases Code on Data Sharing
May 12, 2011

On May 11, 2011, the UK Information Commissioner's Office (the "ICO") published a new statutory code of practice on the sharing of personal data. As stated in the ICO's press release, the code of practice covers best practices for both routine and one-off data sharing activities, and offers organizations tips for reducing the risk of inappropriate or insecure data sharing. By helping organizations understand how to share data appropriately, the code of practice should facilitate compliance with the Data Protection Act and minimize the risk of enforcement actions by the ICO or other regulators. Continue Reading…

Senator Rockefeller Introduces the Do-Not-Track Online Act of 2011
May 9, 2011

On May 9, 2011, Senator Jay Rockefeller (D-WV), the Chairman of the Senate Committee on Commerce, Science and Transportation, introduced the "Do-Not-Track Online Act of 2011" (the "Act"). The Act instructs the Federal Trade Commission to promulgate regulations that would (1) create standards for the implementation of a "Do Not Track" mechanism that would enable individuals to express a desire to not be tracked online and (2) prohibit online service providers from tracking individuals who express such a desire. The regulations would allow online service providers to track individuals who do not want to be tracked only if (1) the tracking is necessary to provide a service requested by the individual (and the individuals' information is anonymized or deleted when the service is provided), or (2) the individual is given clear notice about the tracking and affirmatively consents to the tracking. Continue Reading…

Supreme Court Hears Oral Argument in Sorrell v. IMS Health
May 9, 2011

On April 26, 2011, the United States Supreme Court heard oral argument in *Sorrell v. IMS Health*, a case concerning the constitutionality of a Vermont law that restricts access to prescription drug records. Laws enacted by New Hampshire, Maine and Vermont prohibit pharmacies from selling prescriber-identifiable information in prescription records to third parties for marketing purposes. The Supreme Court seeks to resolve a circuit split that resulted from legal challenges to the statutes in all three states. Thomas Julin, partner at Hunton & Williams LLP, represents IMS Health and discussed the litigation in an interview with Fred Cate, Senior Policy Advisor of the Centre for Information Policy Leadership, during the Centre's First Friday Call on May 6, 2011.

Ceridian and Lookout Services Settle FTC Charges over Failure to Secure Customers' Personal Information
May 5, 2011

On May 3, 2011, the Federal Trade Commission announced that it had reached settlements with Ceridian Corporation and Lookout Services, Inc. after alleging both companies had misrepresented the extent of their data security practices and subsequently failed to safeguard their customers' information. According to the FTC's press release, the settlements "are part of the FTC's ongoing efforts to ensure that companies secure the sensitive consumer information they maintain." Continue Reading…

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