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

June 2012

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:

- Connecticut Amends State Breach Law Amid Introduction of Federal Breach Notification Legislation
- Article 29 Working Party Issues Opinion on Processor Binding Corporate Rules
- FTC and FCC Revising Guidance on Mobile Privacy
- NTIA Launches Development Process for Privacy Code of Conduct for Mobile Apps
- UK ICO Opens Public Consultation on Draft Anonymization Code of Practice
- FTC Announces Settlements Relating to P2P Data Breaches
- FCC Issues Revised Rules Curbing Telemarketing Calls and Text Messages
- Interoperability: Facilitating the Global Flow of Data
- Article 29 Working Party Issues Opinion on Cookie Consent Exemption
- Webcast on Preparing for a New U.S. Privacy Landscape
- FTC Fines Data Broker $800,000 for Alleged FCRA Violations
- Hunton & Williams Maintains Top-Tier Privacy Team Rankings in Chambers USA and The Legal 500 United States
- Massachusetts Hospital Settles Data Breach Lawsuit
- OCR Director Leon Rodriguez Says Tolerance for HIPAA Non-Compliance Is Low
- Vermont Attorney General Announces Amendments to Security Breach Notification Law
- German Government Proposes Amendments to Act on Access to Digital Geographical Data
- Recent Cases Focus Attention on the Video Privacy Protection Act

---

Connecticut Amends State Breach Law Amid Introduction of Federal Breach Notification Legislation
June 27, 2012

In recent weeks, both state and federal regulators have considered security breach notification legislation. On June 15, 2012, Connecticut Governor Dannel Malloy signed a budget bill that, among other things, amends the state's security breach notification law. The changes, which will take effect on October 1, 2012, most notably require businesses to notify the state Attorney General no later than the time when notice of a security breach is provided to state residents. Although the law does not specify when notice must be provided to affected individuals, the law states that such notice must be made "without unreasonable delay," subject to law enforcement delays and the completion of an investigation by the business to determine the nature and scope of the incident, to identify affected individuals, or to restore the reasonable integrity of the data system. As we previously reported, Vermont also recently amended its breach notification statute to require businesses to notify the state Attorney General within 14 days of discovering a security breach or concurrently when notifying consumers, whichever is sooner. Continue reading…

Article 29 Working Party Issues Opinion on Processor Binding Corporate Rules
June 22, 2012

On June 6, 2012, the Article 29 Working Party (the "Working Party") adopted WP 195 (the "Opinion") setting out the requirements for Binding Corporate Rules ("BCRs") for processors. Similar to WP 153, the Opinion lists the requirements to be covered in the processor BCRs application form and the BCRs document itself. The Opinion likely will be welcomed by processors, in particular those that provide large-scale, multinational data processing services. Continue reading…

FTC and FCC Revising Guidance on Mobile Privacy
June 20, 2012

On May 30, 2012, the Federal Trade Commission hosted a public workshop addressing the need for new guidance on advertising and privacy disclosures online and in mobile environments. During the workshop, the FTC announced that it hopes to release an updated version of its online advertising disclosure guidance this fall that would incorporate input from businesses and consumer advocates. Topics explored at the workshop included:

- Best practices for privacy disclosures on mobile platforms and how they can be short, effective and accessible to consumers;
- how to put disclosures in proximity to offers on mobile platforms;
- social media disclosures; and
- the placement of material information on webpages.

Continue reading…

NTIA Launches Development Process for Privacy Code of Conduct for Mobile Apps
June 15, 2012

On June 15, 2012, the National Telecommunications and Information Administration ("NTIA") announced that, in response to a substantial number of comments it received regarding mobile privacy issues, it will convene its first multistakeholder meeting on July 12 to begin the process of developing a code of conduct that promotes transparency in the mobile application context. Continue reading…

UK ICO Opens Public Consultation on Draft Anonymization Code of Practice
June 15, 2012

On May 31, 2012, the UK Information Commissioner's Office ("ICO") published a draft anonymization code of practice (the "Code") which will be open to public consultation until August 23, 2012. The purpose of the Code is to provide organizations with guidance on how personal data can be anonymized successfully, and how to assess the risk of individuals being identified using data that has been anonymized. The ICO also has launched a £15,000 invitation to tender to establish a network of experts to share best practices regarding anonymization. Continue reading…

FTC Announces Settlements Relating to P2P Data Breaches
June 14, 2012

On June 7, 2012, the Federal Trade Commission announced settlement agreements with two businesses that allegedly exposed customers' sensitive personal information by allowing peer-to-peer ("P2P") file-sharing software to be installed on their company computers and networks.

In its complaint against Franklin's Budget Car Sales ("Franklin"), a Georgia automobile dealership that also provides financing services to its customers, the FTC alleged that Franklin failed to implement reasonable security measures to protect the consumer personal information that Franklin routinely collects in connection with its business. The FTC claimed that personal information of approximately 95,000 customers, including names, Social Security numbers, addresses, dates of birth, and drivers' license numbers were made available and disclosed by a P2P application installed on a computer that was connected to Franklin's computer network. In addition to alleging violations of Section 5 of the FTC Act, the FTC also claimed that Franklin violated the Gramm-Leach Bliley Act ("GLB"). This is the first FTC case against an auto dealer involving GLB violations. The FTC stated in its complaint that Franklin failed to implement reasonable security policies and procedures in violation of the GLB Safeguards Rule, and also failed to send consumers annual privacy notices and to provide the required opt-out mechanisms in violation of the GLB Privacy Rule. Continue reading…

FCC Issues Revised Rules Curbing Telemarketing Calls and Text Messages
June 14, 2012

On June 11, 2012, the Federal Communications Commission published in the Federal Register its final revised rules requiring prior express written consent for all autodialed or prerecorded telemarketing "calls" to wireless phones, and for prerecorded telemarking calls to residential lines. The FCC takes the position that the "calls" covered by this written consent requirement include essentially all marketing-oriented text messages. The FCC's rules implement the findings of the Commission's February 2012 Report and Order. Continue reading…

Interoperability: Facilitating the Global Flow of Data
June 14, 2012

As policymakers around the world consider revisions to existing privacy and data protection law, they often refer to "interoperability" as a mechanism to facilitate the flow of data across national and regional borders. Reports released this year by the Obama Administration and the Federal Trade Commission recognize the value of interoperability to the growth of the digital economy and improving privacy compliance. Principles underlying the APEC framework would support a system for transferring data across APEC economies, and the OECD has acknowledged that regulatory authorities worldwide share the responsibility of promoting the protection of cross-border data flows. But although interoperability is expected to help lower barriers to data transfers, simplify compliance and protect individuals' rights, there has been little discussion of how interoperability would work in practice. Continue reading…

Article 29 Working Party Issues Opinion on Cookie Consent Exemption
June 13, 2012

On June 7, 2012, the Article 29 Working Party (the "Working Party") adopted an Opinion analyzing the exemptions to the prior opt-in consent requirement for cookies. Although the Opinion focuses on cookies, the Working Party also notes that the same analysis applies to any technology allowing information to be stored or accessed on a user's computer or mobile device. Continue reading…

Webcast on Preparing for a New U.S. Privacy Landscape
June 13, 2012

On May 24, 2012, Hunton & Williams LLP and Jordan Lawrence Group hosted a webcast on "Preparing for a New U.S. Privacy Landscape: An Overview of the FTC and White House Frameworks." The webcast featured Lisa J. Sotto, partner and head of the Global Privacy and Data Security practice at Hunton &

Williams, Aaron P. Simpson, partner at Hunton & Williams, and Rebecca Perry, Executive Vice President of Professional Services of Jordan Lawrence Group. Listen to the webcast now.

FTC Fines Data Broker $800,000 for Alleged FCRA Violations
June 13, 2012

On June 12, 2012, the Federal Trade Commission announced a settlement agreement with data broker Spokeo, Inc. ("Spokeo"). The FTC alleged that Spokeo operated as a consumer reporting agency and violated the Fair Credit Reporting Act ("FCRA"), and that certain of its advertisements were deceptive in violation of Section 5 of the FTC Act. The proposed settlement order imposes a $800,000 civil penalty on Spokeo and prohibits future violations of the FCRA. This is the first FTC case to address the sale of Internet and social media data in the employment screening context. Continue reading…

Hunton & Williams Maintains Top-Tier Privacy Team Rankings in Chambers USA and The Legal 500 United States
June 8, 2012

Hunton & Williams LLP is pleased to announce its 2012 top rankings from Chambers and Partners and *The Legal 500: United States*. The firm consistently has maintained its number one ranking in both surveys for its Privacy and Data Security practice. Continue reading…

Massachusetts Hospital Settles Data Breach Lawsuit
June 7, 2012

On May 24, 2012, Massachusetts Attorney General Martha Coakley announced that South Shore Hospital agreed to a consent judgment and $750,000 payment to settle a lawsuit stemming from a data breach that occurred in February 2010. At that time, South Shore Hospital shipped several boxes of unencrypted back-up tapes to a service provider in Texas to erase them. The tapes contained the personal and protected health information of approximately 800,000 individuals, including names, Social Security numbers, financial account numbers and medical diagnoses. Several of the boxes went missing and have yet to be recovered, though there is no evidence that the information on the missing tapes has been misused. Continue reading…

OCR Director Leon Rodriguez Says Tolerance for HIPAA Non-Compliance Is Low
June 7, 2012

On June 7, 2012, at the annual Safeguarding Health Information: Building Assurance through HIPAA Security Conference hosted in Washington, D.C. by the Department of Health and Human Services Office for Civil Rights ("OCR") and the National Institute of Standards and Technology ("NIST"), OCR Director Leon Rodriguez said that, given HIPAA's 15-year history and the substantial technical assistance OCR and NIST have provided covered entities, tolerance for HIPAA non-compliance is "much, much lower" than it has been in the past. Continue reading…

Vermont Attorney General Announces Amendments to Security Breach Notification Law
June 7, 2012

On June 1, 2012, the Attorney General of Vermont announced a series of recent legislative moves to enhance the state's consumer protection laws, including amendments to Vermont's security breach notification law. The changes, which were signed into law by Governor Peter Shumlin in early May, include a revised definition of "security breach," the addition of a 45-day timing requirement for notifying

affected consumers, and a requirement to notify the state Attorney General within 14 days of discovering the breach (or when notifying consumers, if sooner). Continue reading…

German Government Proposes Amendments to Act on Access to Digital Geographical Data
June 5, 2012

On May 24, 2012, the German Federal Government submitted to the Parliament (*Bundestag*) a proposal to amend the *Geodatenzugangsgesetz*, a federal law concerning access to geographical data that has been in force since 2009.

The current law implements Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community ("INSPIRE"). In addition to establishing a national geographical data infrastructure, the law aims to provide a legal framework for (1) accessing geographical data, geographical data services and metadata of organizations that maintain such data, and (2) using such data and services, in particular with regard to measures that may affect the environment. The law applies to federal agencies and corporations under public law. Continue reading…

Recent Cases Focus Attention on the Video Privacy Protection Act
June 4, 2012

In recent months, two high-profile cases involving Hulu and Netflix have raised questions regarding the scope and application of the Video Privacy Protection Act ("VPPA"), a federal privacy law that has been the focus of increasing attention over the past few years. In the Hulu case, Hulu users claimed that the subscription-based video streaming service disclosed their viewing history to third parties. Specifically, their complaint alleges that Hulu worked with KISSmetrics, a data analytics company, to track subscribers' viewing histories and then share that information with third parties such as Facebook. In its response, Hulu has maintained that it is not subject to the VPPA because it is not a "video tape service provider," which is defined in relevant part as "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials…" Alternatively, Hulu has argued that its information sharing with third parties was permitted by the VPPA's exception that allows disclosures "incident to the ordinary course of business of the video tape service provider." The case, which currently is headed to mediation, could have far-reaching effects if it is determined that video streaming services are subject to the VPPA's requirements. Continue reading…

Visit our award-winning Privacy and Information Security Law Blog at www.huntonprivacyblog for global privacy and information security law updates and analysis.