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

April 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:

- French Data Protection Authority Unveils Its Agenda for 2012
- Hunton & Williams Privacy Professionals to Speak at the 2012 IAPP Europe Data Protection Intensive
- HHS Finalizes Omnibus HIPAA Rule for OMB Review; Settles with Phoenix Cardiac Surgery Following OCR Investigation
- Canadian Privacy Authorities Release Accountability Guidance
- German Insurance Industry to Establish "Trusted German Insurance Cloud"
- Maryland Legislature Approves Bill Prohibiting Employers from Requesting Social Media Passwords
- Twitter Slaps Spammers with Lawsuit
- Article 29 Working Party Releases Opinion on Facial Recognition Technology
- Centre Files Comments with NTIA to Develop Consumer Privacy Codes of Conduct

---

French Data Protection Authority Unveils Its Agenda for 2012
April 25, 2012

On April 19, 2012, the French Data Protection Authority (the "CNIL") issued a press release detailing its enforcement agenda for 2012. In a report adopted March 29, 2012, the CNIL announced that it will conduct 450 on-site inspections this year, with particular focus on the specific themes described below. The CNIL also indicated that it will continue the work started in 2011 with at least 150 additional inspections related to video surveillance, especially with respect to surveillance in locations that are frequented by large numbers of individuals. Continue reading…

Hunton & Williams Privacy Professionals to Speak at the 2012 IAPP Europe Data Protection Intensive
April 24, 2012

Join Hunton & Williams at the 2012 Europe Data Protection Intensive, now hosted by the International Association of Privacy Professionals ("IAPP") in London, April 25-26, 2012. Hunton & Williams privacy professionals will be featured speakers in the following sessions: Continue reading…

HHS Finalizes Omnibus HIPAA Rule for OMB Review; Settles with Phoenix Cardiac Surgery Following OCR Investigation
April 19, 2012

In the past month, the Department of Health and Human Services ("HHS") sent its final omnibus rule modifying the HIPAA Privacy, Security and Enforcement Rules to the White House Office of Management and Budget ("OMB") and announced a $100,000 settlement with Phoenix Cardiac Surgery, P.C. for violations of the HIPAA Rules. Continue reading…

Canadian Privacy Authorities Release Accountability Guidance
April 18, 2012

On April 17, 2012, the Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioners of Alberta and British Columbia released guidance on their expectations for accountable privacy programs as required by Canadian law. The guidance, entitled "Getting Accountability Right with a Privacy Management Program," discusses the building blocks of a comprehensive privacy program for businesses of all sizes. Although intended for a Canadian audience, the paper likely will have worldwide influence given recent privacy law developments around the globe. Continue reading…

German Insurance Industry to Establish "Trusted German Insurance Cloud"
April 13, 2012

On March 8, 2012, during the CeBIT international IT trade show, the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* or "BSI") accepted the German Insurance Association's application for certification of the "Trusted German Insurance Cloud," a project that aims to establish a secure IT platform for the German insurance industry. The parties previously had agreed to work together to develop practical requirements for a secure cloud solution, and to implement appropriate security measures in the "Trusted German Insurance Cloud." In accordance with the BSI's baseline security parameters, the practical requirements for the cloud are meant to contemplate the ISO 27001 standard as well as appropriate IT security criteria issued by data protection authorities. The implementation of the cloud security requirements will be finalized pursuant to the BSI's certification process.

As was the case when it drafted the position paper "Information Security Issues for Cloud Computing," the BSI has stated that its goal is to work in cooperation with the private sector to develop practical guidelines and recommendations for IT security. The BSI likely will be looking to extend this approach to other industries and sectors by developing a generally applicable certification procedure for cloud services.

Maryland Legislature Approves Bill Prohibiting Employers from Requesting Social Media Passwords
April 12, 2012

On April 9, 2012, Maryland became the first state to pass legislation that would prevent employers from asking or forcing employees and applicants to hand over their social media login credentials. The bill, which passed the state Senate unanimously (Senate Bill 433) and the House of Delegates by a wide margin (House Bill 964), now awaits Maryland Governor Martin O'Malley's signature.

The proposed law would prohibit any "person engaged in a business, an industry, a profession, a trade, or other enterprise in the state, or a unit of State or local government" from requesting or requiring that an employee or applicant disclose any username, password or other means for accessing a personal account or service through an electronic communications device. The Maryland bill also bars employers from firing, disciplining or otherwise penalizing an employee, or failing or refusing to hire an applicant, who refuses to disclose such information. Although the law appears to be relatively broad in scope, critics have noted that it would not prevent employers from "shoulder surfing" to see what employees or applicants have posted online, or from requiring employees to "friend" them on social media sites. Continue reading…

Twitter Slaps Spammers with Lawsuit
April 11, 2012

On April 5, 2012, social media giant Twitter, Inc. ("Twitter") filed a civil lawsuit against spammers and makers of spamming software claiming violations of Twitter's user agreement and various California state and common laws. Borrowing from the popular term for unsolicited email messages, Twitter's complaint describes "spam" on Twitter as "a variety of abusive behaviors" including "posting a Tweet with a harmful link … and abusing the @reply and @mention functions to post unwanted messages to a user." The suit alleges that certain defendants violated Twitter's Terms of Service, which prohibit "spam and abuse," by distributing software tools "designed to facilitate abuse of the Twitter platform and marketed to dupe customers into violating Twitter's user agreement." Other defendants allegedly operated large numbers of automated Twitter accounts through which they attempted to "trick Twitter users into clicking on links to illegitimate websites." Continue reading…

Article 29 Working Party Releases Opinion on Facial Recognition Technology
April 5, 2012

On March 22, 2012, the Article 29 Working Party (the "Working Party"), adopted an Opinion analyzing the privacy and data protection law framework applicable to the use of facial recognition technology in online and mobile services, such as social networks and smartphones. The Working Party defines facial recognition as the "automatic processing of digital images which contain the faces of individuals for the purpose of identification, authentication/verification or categorization of those individuals."

According to the Working Party, a digital image constitutes personal data if it "contains an individual's face which is clearly visible and allows for that individual to be identified." The Working Party further stated that facial recognition reference templates that are stored for comparison purposes in identification and authentication/verification systems constitute personal data, and digital images that are further processed to determine ethnic origin, religion or health information constitute sensitive data. Continue reading…

Centre Files Comments with NTIA to Develop Consumer Privacy Codes of Conduct
April 5, 2012

Drawing on its eleven years of experience facilitating multistakeholder processes, on April 2, 2012, the Centre for Information Policy Leadership at Hunton & Williams LLP filed comments in response to the Department of Commerce's National Telecommunications and Information Administration's request for public comments on the multistakeholder process to develop consumer data privacy codes of conduct. The NTIA's request relates to the topics and processes that will inform the creation of binding codes of conduct as discussed in the Obama Administration's February release of a framework for a Consumer Privacy Bill of Rights.

In its remarks, the Centre indicated support for the multistakeholder approach, but proposed a process that would allow industry stakeholders the opportunity to engage in frank discussions among themselves, without media coverage or concern that their comments might be recorded. While the Centre's proposal emphasized that industry should draft codes of best practices, it also highlighted the need for feedback from experts, advocates and regulators, specifically through a public workshop and written comment period. The Centre also urged the multistakeholder working group to prioritize the development of industry best practices for accountability.

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