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

October 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:

- Israeli Justice Ministry Announces Breakthrough in Information Theft Case
- California Passes Law Prohibiting Discrimination Based on Genetic Information
- Mexico's Ministry of Economy Releases Updated Data Protection Regulations
- California Joins the Growing List of States Restricting Employers' Use of Consumer Credit Reports
- SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents
- New Jersey Courts Issue Conflicting Rulings in ZIP Code Collection Cases
- Council of Europe Considers Proposal to Amend Convention 108 Rules on Transborder Data Flows
- French Data Protection Authority Launches Public Consultation on Cloud Computing
- UK Information Tribunal Rules Properly Anonymized Personal Data Can Be Disclosed Under FOIA
- Centre Presents Accountability Paper at Canadian Privacy Conference
- French Appeals Court Suspends U.S. Company's Whistleblower Program
- Singapore Information Ministry Solicits Comments on Proposed Data Privacy Framework
- Colombian Data Protection Law Approved by Constitutional Court
- German DPAs Issue Resolution and Guidance Paper on Cloud Computing and Compliance with Data Protection Law

---

Israeli Justice Ministry Announces Breakthrough in Information Theft Case
October 27, 2011

On October 24, 2011, Israel's Data Protection Authority, the Israeli Law, Information and Technology Authority in the Israeli Ministry of Justice ("ILITA"), announced significant developments in an information theft case affecting more than nine million Israeli citizens. In 2006, a contract worker hired by Israel's Ministry of Welfare and Social Services downloaded a copy of Israel's population registry to his home computer. The registry later fell into the hands of a software developer and a hacker before being disseminated on the Internet along with a program that allowed users to run searches and queries on the data. The stolen personal information included full names, identification numbers, addresses, dates of birth, dates of immigration to Israel, family status, names of siblings and other information. Continue reading…

California Passes Law Prohibiting Discrimination Based on Genetic Information
October 24, 2011

As reported in the Hunton Employment & Labor Perspectives Blog:

California Governor Jerry Brown recently signed into law Senate Bill No. 559 (SB 559), which prohibits discrimination based on an individual's genetic information. While SB 559 significantly expands the

protections from genetic discrimination provided under the federal Genetic Information Nondiscrimination Act of 2008 (GINA), at this time, its impact on most California employers is thought to be limited to the potential for greater damages to be awarded under it than under its federal counterpart. Continue reading…

Mexico's Ministry of Economy Releases Updated Data Protection Regulations
October 21, 2011

On October 20, 2011, Mexico's Ministry of Economy made public an update to its proposed Regulations to the Federal Law for the Protection of Personal Data Held by Private Parties. The new draft regulations, which contain changes made in light of public comments on the prior version, will take effect if they receive final executive approval, which may happen later this year. The updates to the draft regulations include:

- Rules specific to cloud computing
- Clarification of notice requirements
- Clarification of consent requirements
- Exemptions for certain business contact information
- Revisions to data transfer restrictions
- Updated security and breach notification provisions
- Revised requirements for self-regulatory schemes
- Revisions to provisions governing the exercise of data subjects' rights

California Joins the Growing List of States Restricting Employers' Use of Consumer Credit Reports
October 21, 2011

As reported in the Hunton Employment & Labor Perspectives Blog, on October 10, 2011, California became the seventh state to enact legislation restricting public and private employers alike from using consumer credit reports in making hiring and other personnel decisions. Assembly Bill No. 22 both adds a new provision to the California Labor Code — Section 1024.5 — and amends California's Consumer Credit Reporting Agencies Act ("CCRAA"). Effective January 1, 2012, California employers will be prohibited from requesting a consumer credit report for employment purposes unless they meet one of the limited statutory exceptions, and those employers meeting an exception, will be subjected to increased disclosure requirements. Connecticut, Illinois, Hawaii, Oregon, Maryland and Washington already have similar laws on the books, and many other states, as well as the federal government, are contemplating similar legislation. This trend creates a potential "credit-centric" minefield for employers that do business in any one or more of these states. In light of the multiple laws affecting their use, employers who utilize consumer credit reports in making personnel decisions should proceed cautiously. Employers must evaluate the need for these reports in making personnel decisions, review and modify their policies to ensure compliance with the myriad of regulations in this area, and monitor any new developments to ensure continued compliance. Continue reading…

SEC Issues Disclosure Guidance on Cybersecurity Matters and Cyber Incidents
October 20, 2011

On October 13, 2011, the Securities and Exchange Commission Division of Corporation Finance issued disclosure guidance ("Guidance") regarding cybersecurity matters and cyber incidents. While the Guidance does not change existing disclosure requirements, it does add specificity to existing requirements. In some respects, that specificity is helpful, but the Guidance fails to take into account the uncertainty that inevitably accompanies efforts to assess and disclose cybersecurity matters and incidents.

Read a detailed summary of the Guidance and analysis regarding its effects, including its impact on disclosures both before and after a cyber incident, enforcement-related proceedings and potential litigation.

New Jersey Courts Issue Conflicting Rulings in ZIP Code Collection Cases
October 18, 2011

Last month, two New Jersey judges issued opposing decisions in class action lawsuits regarding merchants' point-of-sale ZIP code collection practices. The conflicting orders leave unanswered the question of whether New Jersey retailers are prohibited from requiring and recording customers' ZIP codes at the point of sale during credit card transactions. Continue reading…

Council of Europe Considers Proposal to Amend Convention 108 Rules on Transborder Data Flows
October 17, 2011

On October 10-12, 2011, the Council of Europe's Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (known as the "T-PD-Bureau") met in Strasbourg, France, to discuss, among other things, amending the Council of Europe's Convention 108 and Additional Protocol. Convention 108 (together with the Protocol), which underlies the European Union's legal framework for data protection, is the only legally-binding international convention that addresses data protection. Amendment of the Convention is also closely linked to the current review of the EU data protection framework. Continue reading…

French Data Protection Authority Launches Public Consultation on Cloud Computing
October 17, 2011

On October 17, 2011, the French Data Protection Authority (the "CNIL") launched a public consultation on cloud computing (the "Consultation"). The Consultation seeks to gather opinions from stakeholders (clients, providers, consultants) regarding cloud computing services for businesses, to identify legal and technical solutions that address data protection concerns while taking into account the economic interests involved. Continue reading…

UK Information Tribunal Rules Properly Anonymized Personal Data Can Be Disclosed Under FOIA
October 14, 2011

On September 7, 2011, the United Kingdom Information Tribunal published a decision that appears to resolve the long-running uncertainty regarding the extent to which anonymized personal information may be disclosed under the UK's Freedom of Information legislation. The UK's FOIA was introduced and

applicable to most of the UK in 2000, with equivalent law following for Scotland in 2002. Continue reading…

Centre Presents Accountability Paper at Canadian Privacy Conference
October 13, 2011

On October 13, 2011, Marty Abrams, President of the Centre for Information Policy Leadership at Hunton & Williams LLP, presented "Accountability in a Page" as part of the "What it Means to Be Accountable" plenary session at the PIPA Conference 2011 taking place in Vancouver, British Columbia. Mr. Abrams, who leads the Centre's Accountability Project, outlined the essential elements of accountability and described how top multinational companies are building accountability-based programs. According to Mr. Abrams, "accountability as mandated by the Canadian private sector privacy law requires companies to have comprehensive programs that include polices, mechanisms to put those policies into effect, and review processes to assure the mechanisms are functional." Mr. Abrams provided attendees with a one-pager on accountability that includes a list of common elements companies are using to implement accountability programs.

For more information on accountability, visit the Centre's website on the Accountability Project.

French Appeals Court Suspends U.S. Company's Whistleblower Program
October 13, 2011

On September 23, 2011, the Labor Chamber of the Court of Appeals of Caen (the "Court") upheld a decision to suspend a whistleblower program implemented by a U.S. company's French affiliate, despite the fact that the French Data Protection Authority (the "CNIL") had inspected and approved the program prior to implementation. This decision follows recent amendments to the legal framework for whistleblower programs in France. Continue reading…

Singapore Information Ministry Solicits Comments on Proposed Data Privacy Framework
October 11, 2011

On September 13, 2011, the Singapore Ministry of Information, Communications and the Arts (the "Ministry") published a Proposed Consumer Data Protection Regime for Singapore, outlining possible ideas for a data privacy framework and soliciting comments from the public. A few of the suggestions from the Ministry's proposal that appear most likely to be reflected in a final data privacy law are outlined below.

- The proposed framework would provide a baseline applicable to all private sector organizations, to ensure universal minimum standards for the protection for personal data.
- More stringent protections that exceed the basic minimum requirements may be implemented for particular industry sectors.
- Public sector organizations would continue to be bound by the existing framework applicable to them, and would not be subject to the new framework.
- Disclosure of personal information, and possibly also collection and processing of personal information, would require the informed consent of individual data subjects.
- The framework should be drafted so as to enhance and preserve Singapore's status as an international business center and a principal location for global data management and processing services.

Continue reading…

Colombian Data Protection Law Approved by Constitutional Court
October 10, 2011

On October 7, 2011, the Constitutional Court of Colombia approved a landmark omnibus data protection law. According to its press release, the Court approved almost all provisions in the legislation, known as *Ley estatutaria No. 184/ 10 Senado, 046/10 Cámara*, but it took issue with Article 27 (which addresses the government's processing of certain data), Article 29 (which addresses the expunging of certain criminal records) and Articles 30 and 31 (which both address intelligence and counterintelligence databases). Many of the remaining provisions reflect a strong European influence. Some highlights include:

- With certain exceptions, the law prohibits the processing of personal data without the data subject's prior consent. When the personal data are sensitive data (e.g., health data), the consent must take the form of an explicit authorization.

- The law permits cross-border transfers of personal data to countries that lack adequate data protection laws only in specified circumstances, such as (1) when the data subject has given express and unequivocal consent for the transfer (2) the transfer is necessary for the performance of a contract between the data subject and the data controller, or (3) with the approval of the Superintendence of Industry and Commerce.

- The processing of children's personal data is generally prohibited.

- Data subjects have access rights.

Continue reading…

German DPAs Issue Resolution and Guidance Paper on Cloud Computing and Compliance with Data Protection Law
October 5, 2011

On September 29, 2011, the German federal and state data protection authorities ("DPAs") issued a resolution on cloud computing and compliance with data protection law. The publication was released in conjunction with the DPAs' 82nd annual conference.

In the resolution, the DPAs ask that cloud service providers ensure their services comply with data protection law, and cloud service customers are urged to use cloud services only if they are in a position to fulfill their obligations as data controllers and have verified that the appropriate data protection and information security requirements are in place. The DPAs state that, in addition to ensuring the confidentiality, integrity and availability of data, data controllers must take into account the difficult-to-implement requirements concerning control, transparency and influence over data processing. According to the DPAs, deploying cloud computing solutions should not relieve data controllers, particularly management, of their responsibilities with respect to their data processing operations. 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.