CLIENT ALERT

HUNTON& WILLIAMS

June 2010

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:

- Article 29 Working Party Calls on FTC to Investigate Online Retention and Anonymization Policies
- FTC Further Extends Enforcement Deadline for Red Flags Rule
- FTC Investigating Privacy Risks to Data Stored on Digital Copiers
- HHS To Examine Breach Notification and Risk Mitigation Plans
- Russia Considers Improving its Data Protection Law
- HHS Official Reports Uptick in HIPAA Security Rule Enforcement
- Uncertainty Reigns Supreme: What Impact Will a Coalition Government Have on Data Protection Law in the UK?
- EU Agency for Fundamental Rights: Prosecutions and Sanctions for Violations of Data Protection Law Limited or Non-Existent
- Commerce Department Takes Lead in Developing U.S. Internet Privacy Framework
- State Law Trumps HIPAA in Suit Over Disclosure of Medical Records
- U.S. Legislators Urge Enhanced Privacy Protections for Social Networking Websites
- Mexican Senate Approves Data Protection Bill

Article 29 Working Party Calls on FTC to Investigate Online Retention and Anonymization Policies

June 1, 2010

In a letter to the U.S. Federal Trade Commission dated May 26, 2010, the Article 29 Working Party expressed concerns regarding the retention and anonymization policies of Google, Yahoo! and Microsoft. Specifically, the Working Party requested that the FTC examine the compatibility of the three search engine providers' actions with provisions of Section 5 of the FTC Act which prohibits unfair or deceptive trade practices. Continue Reading…

FTC Further Extends Enforcement Deadline for Red Flags Rule

May 28, 2010

On May 28, 2010, the FTC announced that it would again delay enforcement of the Identity Theft Red Flags Rule. This is the fifth time the Commission has announced an extension of the enforcement deadline, after most recently extending the deadline to June 1, 2010. The Red Flags Rule requires "creditors" and "financial institutions" that have "covered accounts" to develop and implement written identity theft prevention programs to help identify, detect and respond to patterns, practices or specific activities – known as "red flags" – that could indicate identity theft. The enforcement date is now December 31, 2010, for creditors and financial institutions subject to FTC jurisdiction. The FTC stated that the delay had been requested by members of Congress who are currently considering a bill that would limit the rule's scope. If Congress passes legislation limiting the scope of the Red Flags Rule with

an effective date earlier than December 31, 2010, the FTC will begin enforcement as of that effective date.

Please refer to our previous post regarding other developments that may limit the Red Flags Rule's application.

FTC Investigating Privacy Risks to Data Stored on Digital Copiers
May 26, 2010

Federal Trade Commission Chairman Jon Leibowitz recently sent a letter to Congressman Edward Markey, Co-Chairman of the bipartisan Congressional Privacy Caucus, announcing that the FTC will addresses the privacy risks associated with the use of digital copiers. Congressman Markey had had urged the FTC to investigate this issue after a CBS News exposé showed that almost every digital copier produced since 2002 stores on its hard drive images of documents that are "scanned, copied or emailed by the machine" – including documents with sensitive personal information. Continue Reading…

HHS To Examine Breach Notification and Risk Mitigation Plans
May 24, 2010

The Office for Civil Rights ("OCR") within the Department of Health and Human Services ("HHS") has announced that it will more closely examine covered entities' breach notification and risk mitigation plans. OCR noted that small and medium sized covered entities have been particularly vulnerable to data breaches. The National Institute for Standards and Technology ("NIST") will publish a guide for covered entities that "outlines the steps to mitigate risks for data breaches, training for how to respond to breaches, and overall preparation in the event of a breach, such as alternate storage facilities for data."

As previously discussed on this blog, OCR has announced an uptick in HIPAA Security Rule enforcement and issued draft guidance regarding the "risk analysis" implementation specification in the Security Rule.

Russia Considers Improving its Data Protection Law
May 21, 2010

The Russian Federation is considering amending the country's data protection law, according to BNA's Privacy Law Watch. Businesses have long complained that the law contains restrictions on data processing that are extremely difficult to meet. For example, the law requires affirmative written consent for most types of data processing. In the online context, this provision has been interpreted to require a consumer's digital signature. A check box, which is an acceptable mechanism for expressing consent in the EU, for example, is deemed unacceptable in Russia. In practice, this and other requirements of the data protection law have been widely ignored, even by Russia's biggest Internet businesses. Not surprisingly, Russia's data protection regulator – the Russian Federal Service for Oversight of Communications, Information Technology and Mass Media ("Roscomnadzor") – has found the rate of noncompliance with the law to be high. Roscomnadzor has reported that over 400 audits conducted in 2009 revealed 86 incidents of noncompliance. In connection with the proposed amendments to the law, the regulator already has received over 100 recommendations from businesses and data protection professionals aimed at improving the law and implementing regulations.

HHS Official Reports Uptick in HIPAA Security Rule Enforcement
May 14, 2010

David Holtzman, a health information privacy specialist at the Office for Civil Rights ("OCR") within the Department of Health and Human Services ("HHS"), stated at a health privacy conference on May 11,

2010, that OCR has been "vigorously" enforcing the Security Rule, which was promulgated pursuant to the Health Insurance Portability and Accountability Act ("HIPAA"). Prior to 2009, HHS divided civil enforcement responsibility for HIPAA between OCR, which enforced the HIPAA Privacy Rule, and the Centers for Medicare and Medicaid Services ("CMS"), which enforced the HIPAA Security Rule. In July 2009, the Secretary of HHS delegated authority to enforce the HIPAA Security Rule to OCR to "facilitate improvements by eliminating duplication and increasing efficiency." Continue Reading…

Uncertainty Reigns Supreme: What Impact Will a Coalition Government Have on Data Protection Law in the UK?

May 13, 2010

Following the first "hung parliament" since 1974, the UK is facing considerable legislative reform under the newly formed Conservative - Liberal Democrat coalition government. Although the parties appear to have differing opinions on a number of legislative issues, one issue that unites them is their commitment (at least in theory) to strengthening the current data protection regime implemented under the Labour government.

Each party's manifesto states that, should it be elected, it will enhance the audit powers of the Information Commissioner (the UK data protection regulator). Currently, the Information Commissioner may audit government departments and public authorities suspected of violating data protection principles without their prior consent. The Conservatives and Liberal Democrats propose to extend the Information Commissioner's audit powers to private sector organizations. This could be achieved in theory by secondary legislation. Continue Reading…

EU Agency for Fundamental Rights: Prosecutions and Sanctions for Violations of Data Protection Law Limited or Non-Existent
May 12, 2010

According to a report issued by the EU Agency for Fundamental Rights ("FRA"), European data protection authorities lack sufficient independence and funding. In addition, DPAs impose few sanctions for violations of data protection laws. DPAs "are often not equipped with full powers of investigation and intervention or the capacity to give legal advice or engage in legal proceedings." In a number of countries, including Austria, France, Germany, Latvia, the Netherlands, Poland and the UK, "prosecutions and sanctions for violations are limited or non-existing." The report also highlights EU citizens' limited awareness of the DPAs' existence. The FRA Director, Morten Kjaerum, noted that "improvements need to take place concerning the independence, effectiveness, resources and powers of data protection authorities."

Commerce Department Takes Lead in Developing U.S. Internet Privacy Framework
May 11, 2010

"The Department of Commerce is back." With those words Cameron Kerry, General Counsel of the U.S. Department of Commerce, made it clear the Department intends to take a leading role in shaping domestic privacy policy and representing U.S. privacy interests in international discussions. The announcement was made at the May 7, 2010, Department of Commerce symposium, "A Dialogue on Privacy and Innovation," where the mostly business audience welcomed Mr. Kerry's declaration with great enthusiasm. Continue Reading…

State Law Trumps HIPAA in Suit Over Disclosure of Medical Records
May 7, 2010

Rejecting a defense based on compliance with the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), a federal court in Ohio denied a medical clinic's motion to dismiss invasion of privacy claims following the clinic's disclosure of medical records to a grand jury. In *Turk v. Oiler,* No. 09-CV-381 (N.D. Ohio Feb. 1, 2010), plaintiff Turk had been under investigation for illegally carrying a concealed weapon and for having a weapon while under disability in violation of an Ohio law which provides that "no person shall knowingly acquire, have, carry, or use any firearm" if "[t]he person is drug dependent, in danger of drug dependence, or a chronic alcoholic." Defendant Cleveland Clinic, where Turk was a patient, received a grand jury subpoena requesting "medical records to include but not be limited to drug and alcohol counseling and mental issues regarding James G. Turk." When the Cleveland Clinic disclosed Turk's medical records in response to this subpoena, Turk sued the clinic for violating his privacy rights. Continue Reading…

U.S. Legislators Urge Enhanced Privacy Protections for Social Networking Websites
April 29, 2010

Legislators at the federal and state levels are urging social networking websites to enhance privacy protections available to their users. On April 27, 2010, four U.S. Senators wrote a letter to Facebook's CEO expressing "concern regarding recent changes to the Facebook privacy policy and the use of personal data on third party websites." The letter urged Facebook to provide opt-in mechanisms for users, as opposed to lengthy opt-out processes, and highlighted default sharing of personal information, third-party advertisers' data storage and instant personalization features as three areas of concern. Continue Reading…

Mexican Senate Approves Data Protection Bill
April 29, 2010

The Mexican Senate has unanimously approved a landmark data protection law governing information use in the private sector, *la Ley Federal de Protección de Datos Personales en posesión de los particulares* (full text in Spanish). We provided information on the bill last week when the Chamber of Deputies voted to approve it. The legislation has been forwarded to the president for signature. We will provide further details as this story develops.

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