

July 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:

- [Coalition of States Demands Answers About Google Street View](#)
- [Sweeping Privacy Legislation Would Include Private Right of Action](#)
- [German Federal Office for Information Security Issues Document on Data Protection and RFID](#)
- [Ukraine Adopts a New Data Protection Law](#)
- [Article 29 Working Party Provides Opinion on Accountability to the European Commission](#)
- [FTC's David Vladeck Opposes Bankruptcy Transfer of Personal Information](#)
- [Irish Government Challenges Adequacy Level of Data Protection in Israel](#)
- [UK Information Commissioner's Office Launches New Code of Practice](#)
- [Mexico's Data Protection Law Now in Effect](#)
- [HHS Issues Modifications to the HIPAA Privacy, Security and Enforcement Rules](#)
- [Facebook Announces Privacy Changes for Third-Party Applications](#)

---

## **Coalition of States Demands Answers About Google Street View July 22, 2010**

On July 21, 2010, a coalition of 38 states sent a letter to Google demanding more information about the company's collection of data from unsecured wireless networks by its Google Street View vehicles. The letter was sent by Connecticut Attorney General Richard Blumenthal on behalf of the executive committee of a multistate working group investigating Google Street View practices. [As we reported on June 22](#), Blumenthal has spearheaded the nationwide investigation into Google Street View. Among other things, the letter asks Google to identify who was responsible for the software code that allowed the Street View cars to collect data broadcast over Wi-Fi networks, and for a list of states where unauthorized data collection occurred. The letter also asks Google for details regarding whether any of the data was disclosed to third parties or used for marketing purposes. [Continue Reading...](#)

## **Sweeping Privacy Legislation Would Include Private Right of Action July 20, 2010**

On July 19, 2010, Representative Bobby Rush (D-Ill.) [introduced a bill](#) "to foster transparency about the commercial use of personal information" and "provide consumers with meaningful choice about the collection, use and disclosure of such information." The bill, cleverly nicknamed the "BEST PRACTICES Act", presumably intends to set the standards for the use of consumer personal information by marketers. A similar bill [was introduced by Representatives Boucher and Stearns in early May](#). Although both proposals would require opt-out consent for online behavioral advertising and express, affirmative consent for the collection or sharing of sensitive information, Rush's bill has a broader definition of "sensitive information" and includes several other key differences. Perhaps most notably, unlike the

earlier draft legislation, Rush's bill features a private right of action that would allow individuals to sue companies that violate the law for up to \$1,000 in actual damages, plus punitive damages and costs and attorney's fees. The bill contains a safe harbor from the private right of action for companies that participate in, and comply with, a self-regulatory "Choice Program" approved by the FTC. In addition, the bill excludes from its definition of "covered information" any information collected from or about an employee by an employer "that directly relates to the employee-employer relationship." A hearing on the proposed bill will be held on Thursday July 22, 2010.

[Read the text of the bill.](#)

## **German Federal Office for Information Security Issues Document on Data Protection and RFID**

**July 20, 2010**

On July 7, 2010, the German Federal Office for Information Security, the [Bundesamt für Sicherheit in der Informationstechnik](#) ("BSI"), published a basic paper on data security and data protection for radio-frequency identification ("RFID") applications. The paper, [Technical Guidelines RFID as Templates for the PIA-Framework](#), describes how to use RFID in compliance with data protection requirements, and explains the relationship between the BSI's [technical guidelines](#) for the secure use of RFIDs and the European Commission's Privacy Impact Assessment ("PIA") Framework. [Continue Reading...](#)

## **Ukraine Adopts a New Data Protection Law**

**July 20, 2010**

On June 1, 2010, Ukraine's parliament adopted a [bill](#) on the protection of personal data which introduces a comprehensive regulatory regime for data processing in the country. The bill was signed by the President of Ukraine on June 24, 2010, and will come into force on January 1, 2011. [Continue Reading...](#)

## **Article 29 Working Party Provides Opinion on Accountability to the European Commission**

**July 16, 2010**

The European Union's Article 29 Working Party adopted a [detailed recommendation](#) on accountability which was submitted to the European Commission on July 13, 2010. Opinion 3/2010 elaborates on the Working Party's 2009 recommendation to include a new principle on accountability in the revised EU Data Protection Directive. The Opinion's executive summary states:

*"EU data protection principles and obligations are often insufficiently reflected in concrete internal measures and practices. Unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data mishaps are likely to continue. ...this Opinion puts forward a concrete proposal for a principle on accountability which would require data controllers to put in place appropriate and effective measures to ensure that principles and obligations set out in the Directive are complied with, and to demonstrate so to supervisory authorities upon request."*

[Continue Reading...](#)

## **FTC's David Vladeck Opposes Bankruptcy Transfer of Personal Information**

**July 15, 2010**

David Vladeck, Director of the FTC's Bureau of Consumer Protection, recently sent a [letter](#) to creditors of XY Magazine, warning that the creditors' acquisition of personal information about the debtor's

subscribers and readers in contravention of the debtor's privacy promises could violate the Federal Trade Commission Act ("FTC Act"). [Continue Reading...](#)

## **Irish Government Challenges Adequacy Level of Data Protection in Israel** **July 9, 2010**

On July 6, 2010, the Irish government formally objected to the adequacy procedure initiated by the European Commission that would have allowed the free flow of European personal data to Israel, over concerns of the possible use of the information by Israeli officials. This political move follows recent revelations regarding forgery of European passports, including several from Ireland, and their alleged use by Israel's intelligence services. [Continue Reading...](#)

## **UK Information Commissioner's Office Launches New Code of Practice** **July 9, 2010**

On July 7, 2010, the UK Information Commissioner's Office published a [new code of practice](#) for the collection of personal data online. Launching the new code at a data protection conference, UK Information Commissioner Christopher Graham said, "the benefits of the internet age are clear: the chance to make more contacts, quicker transactions and greater convenience. But there are risks too. A record of our online activity can reveal our most personal interests. Get privacy right and you will retain the trust and confidence of your customers and users; mislead consumers or collect information you don't need and you are likely to diminish customer trust and face enforcement action from the ICO." [Continue Reading...](#)

## **Mexico's Data Protection Law Now in Effect** **July 8, 2010**

On July 6, 2010, Mexico's [Ley Federal de Protección de Datos Personales en Posesión de los Particulares](#) came into force. As we [previously reported](#), on April 27, 2010, the Mexican Senate unanimously approved this landmark federal data protection law governing the collection, processing and disclosure of personal data by the private sector. Pursuant to the adoption of the new law, the Mexican Federal Institute of Access to Public Information has changed its name to the [Federal Institute of Access to Information and Data Protection](#).

[As reported by the IAPP](#), the Institute's oversight powers will now include regulation of the private sector in addition to having authority with respect to government entities. The new law contemplates the rights of existing regulatory authorities to issue regulations in conjunction with the Institute, with non-compliance by a data controller being addressed first by the relevant industry regulator.

## **HHS Issues Modifications to the HIPAA Privacy, Security and Enforcement Rules** **July 8, 2010**

On July 8, 2010, the Department of Health and Human Services ("HHS") issued a notice of proposed rulemaking to modify the Privacy, Security and Enforcement Rules promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996. The modifications implement changes made by the Health Information Technology for Economic and Clinical Health Act (the "HITECH" Act) enacted in 2009. [Continue Reading...](#)

## Facebook Announces Privacy Changes for Third-Party Applications July 1, 2010

Bret Taylor, the Chief Technology Officer of Facebook, announced this week on the [Facebook Blog](#) that the company will enhance privacy protections pertaining to third-party applications. When a Facebook user logs into a third-party application with his or her Facebook account, the application will only be able to access the public parts of the user's Facebook profile. If the application wants to access private sections of a user's Facebook profile, the application has to explicitly ask the Facebook user for permission. For example, if a greeting card application wants to access a user's photos to create a personalized greeting card, the Facebook user will have to click a button to allow such access.

In his announcement, Mr. Taylor stated that the changes "reflect two core Facebook beliefs: first, your data belongs to you; second, it should be easy to control what you share. If at any point you ask a developer to remove the data you've granted them access to, we require that they delete this information." The changes come in the wake of scrutiny by both [legislators](#) and [privacy organizations](#) regarding privacy protections on the social networking website.



Visit the Privacy and Information Security Law Blog at [www.huntonprivacyblog](http://www.huntonprivacyblog) for global privacy and information security law updates and analysis.