

February 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:

- [Digital Advertising Alliance Supports Browser-Based Choice Mechanism](#)
- [American Bar Association Asks Courts to Consider Foreign Privacy Laws](#)
- [White House Announces Its Highly Anticipated Consumer Privacy Bill of Rights](#)
- [Senators Introduce Cybersecurity Act of 2012](#)
- [FTC Issues "Warning Call" to Developers of Apps for Kids](#)
- [European Court of Justice Sets Criteria for Balancing Privacy Rights and Copyrights in the Social Networking Context](#)
- [Hong Kong Privacy Commissioner Offers Guidance for Complying with Data Privacy Ordinance](#)
- [Article 29 Working Party Issues Guidance on European Patients Smart Open Services](#)
- [UK Ministry of Justice Opens Call for Evidence on European Commission's Proposed Regulation and Directive](#)
- [UK ICO Issues Revised Guidance on Fines](#)
- [FTC Warns Marketers of Mobile Apps About Potential FCRA Violations](#)
- [Hunton & Williams Partner Publishes Comprehensive Analysis of EU Data Protection Regulation Reform Proposal](#)
- [UK ICO Encourages Voluntary Data Protection Audits and Advisory Visits](#)
- [UK and U.S. Regulators Introduce New Breach Guidance, Notification Forms](#)
- [Chinese Ministry of Industry and Information Technology Issues New Data Protection Regulations](#)
- [German DPAs Comment on Proposed EU Data Protection Law Reform](#)

Digital Advertising Alliance Supports Browser-Based Choice Mechanism February 28, 2012

The Digital Advertising Alliance ("DAA") recently [announced](#) that its members will work "to add browser-based header signals to the set of tools by which consumers can express their preferences" not to be tracked online and will work with browser providers to develop "consistent language across browsers...that describes to consumers the effect of exercising such choice."

This announcement came on the heels of the Obama administration's [release](#) of a framework for a Consumer Privacy Bill of Rights. The DAA's agreement represents the industry's attempt to appease consumer privacy concerns in the face of the growth of online advertising. The DAA represents over 400 advertising and technology companies. [Continue reading...](#)

American Bar Association Asks Courts to Consider Foreign Privacy Laws February 24, 2012

The American Bar Association's ("ABA's") House of Delegates adopted a non-binding [resolution](#) urging courts to consider foreign data protection and privacy laws when resolving discovery issues. The full text of the resolution is as follows:

"RESOLVED, That the American Bar Association urges that, where possible in the context of the proceedings before them, U.S. federal, state, territorial, tribal and local courts consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation."

[Continue reading...](#)

White House Announces Its Highly Anticipated Consumer Privacy Bill of Rights February 23, 2012

The White House today released its long-awaited report outlining a framework for U.S. data protection and privacy policy. As expected, "[Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Global Innovation in the Global Digital Economy](#)" articulates a Consumer Privacy Bill of Rights based on the individual's right to exercise control over what personal data companies collect from the individual and how companies use the data. The Consumer Privacy Bill of Rights, which reflects principles of fair information practices and applies to personal data, sets forth individual rights for consumers and corresponding obligations of companies in connection with personal data. It also provides for the consumer's right to:

- transparent privacy and data security practices;
- expect that companies will collect, use and disclose data in a manner consistent with the context in which it was collected;
- have their data handled in a secure manner;
- access and correct personal data;
- set reasonable limits on the personal data that companies collect and retain; and
- have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

[Continue reading...](#)

Senators Introduce Cybersecurity Act of 2012 February 22, 2012

On February 14, 2012, a joint U.S. congressional committee, including Senators Joseph Lieberman (I-CT), Susan Collins (R-ME), Jay Rockefeller (D-WV) and Dianne Feinstein (D-CA), [introduced](#) the [Cybersecurity Act of 2012](#) (the "Act"). Although the legislation appears to have strong bipartisan support, during a February 15 hearing before the Homeland Security and Governmental Affairs Committee, Senator John McCain (R-AZ) indicated that he and six Republican colleagues would propose their own cybersecurity legislation in March. [Continue reading...](#)

FTC Issues "Warning Call" to Developers of Apps for Kids February 21, 2012

In its new report, [Mobile Apps for Kids: Current Privacy Disclosures are Disappointing](#), the Federal Trade Commission issues a "warning call to industry that it must do more to provide parents with easily accessible, basic information about the mobile apps that their children use." The report indicates:

“Parents should be able to learn what information an app collects, how the information will be used, and with whom the information will be shared. App developers also should alert parents if the app connects with any social media, or allows targeted advertising to occur through the app. Third parties that collect user information through apps also should disclose their privacy practices, whether through a link on the app promotion page, the developers’ disclosures, or another easily accessible method.”

[Continue reading...](#)

European Court of Justice Sets Criteria for Balancing Privacy Rights and Copyrights in the Social Networking Context February 17, 2012

On February 16, 2012, the European Court of Justice held in the *SABAM vs. Netlog* case ([C-360/10](#)) that imposing an obligation on social networks to install a “general filtering system” to prevent all users from sharing copyrighted music is disproportionate to the extent that such filters may infringe on user privacy rights or block lawful communications. *SABAM*, a Belgian copyright association, had filed an injunction against social network provider Netlog that would have required Netlog to install filtering systems to prevent copyright infringements by Netlog users. The Belgian court deciding on the injunction requested a preliminary ruling from the ECJ. [Continue reading...](#)

Hong Kong Privacy Commissioner Offers Guidance for Complying with Data Privacy Ordinance February 16, 2012

Since October 2011, the Hong Kong [Office of the Privacy Commissioner for Personal Data](#) has published three “Guidance Notes” to help data users comply with the [Personal Data \(Privacy\) Ordinance](#) (the “Ordinance”). These Notes are not legally binding, nor are they intended to serve as an exhaustive guide to the application of the Ordinance, but they provide good, practical examples and tips that the Commissioner has developed as it has implemented the Ordinance. [Continue reading...](#)

Article 29 Working Party Issues Guidance on European Patients Smart Open Services February 14, 2012

On January 25, 2012, the [Article 29 Working Party](#) (the “Working Party”) issued a [Working Document](#) providing guidance on data protection issues relating to the [European Patients Smart Open Services](#) (“epSOS”) project. epSOS is a pilot project focused on developing an information and communications technology infrastructure that enables access to patient health information (i.e., Patient Summaries) among different EU Member States for the purpose of providing medical treatment. The project also aims to facilitate the cross-border use of electronic prescriptions (i.e., ePrescriptions). epSOS involves the collaboration of a significant number of [health care provider organizations](#) and [companies](#) that contribute their knowledge and expertise to the project. [Continue reading...](#)

UK Ministry of Justice Opens Call for Evidence on European Commission’s Proposed Regulation and Directive February 7, 2012

On February 7, 2012, the UK Ministry of Justice [launched](#) its Call for Evidence on the European Commission’s proposed general data protection regulation and criminal justice data protection directive (the “Proposals”). The Ministry is looking to gain perspective and solicit feedback on how the Proposals likely would impact organizations and individuals in the UK. [Continue reading...](#)

UK ICO Issues Revised Guidance on Fines February 7, 2012

Monetary penalties are one mechanism in a suite of tools that the UK Information Commissioner's Office ("ICO") uses to encourage compliance with data protection regulations. The ICO generally uses monetary penalties to sanction deliberate or negligent breaches of the law, but the purpose is not to impose financial hardship but rather to "act as an encouragement towards compliance, or at least as a deterrent against non-compliance." The following is a brief overview of the ICO's authority to issue monetary penalties. [Continue reading...](#)

FTC Warns Marketers of Mobile Apps About Potential FCRA Violations February 6, 2012

On February 6, 2012, the Federal Trade Commission [warned](#) six marketers of background screening mobile applications that they may be violating the Fair Credit Reporting Act ("FCRA"). In a [sample letter](#) posted on the FTC website, the FTC indicates that at least one of the recipient marketer's mobile apps involves background screening reports that include criminal history checks. Pursuant to the FCRA, this could make the marketers of the mobile apps "consumer reporting agencies" if they are "providing information to employers regarding current or prospective employees' criminal histories [that] involves the individuals' character, general reputation, or personal characteristics." [Continue reading...](#)

Hunton & Williams Partner Publishes Comprehensive Analysis of EU Data Protection Regulation Reform Proposal February 6, 2012

[Christopher Kuner](#), partner in the Brussels office of Hunton & Williams, has published an [article providing an exhaustive analysis](#) of the European Commission's proposed Data Protection Regulation reform package, which was [released on January 25, 2012](#). The article, which appears in the February 6 issue of the [BNA Privacy Law Watch](#), discusses the background and genesis of the proposal, analyzes the provisions of greatest interest to the private sector, and draws conclusions about the proposed reform package's impact and future as it enters the EU legislative process.

Read the full text of Kuner's article, [The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law](#).

UK ICO Encourages Voluntary Data Protection Audits and Advisory Visits February 3, 2012

Throughout 2011, the UK Information Commissioner's Office ("ICO") escalated its use of data protection audits, encouraging organizations to submit to voluntary audits and seeking to increase its ability to conduct compulsory audits. Currently, the ICO has the authority to compel central government departments to undergo audits, but it would like to [extend compulsory audits](#) to include local government, the national health service and the private sector. [Continue reading...](#)

UK and U.S. Regulators Introduce New Breach Guidance, Notification Forms February 3, 2012

In recent weeks, regulators in California and Illinois have issued guidance on responding to data security breaches, while UK and California authorities released online forms for organizations to use when providing notification of a breach to regulators.

In December 2011, the UK Information Commissioner's Office ("ICO") released a new [breach notification form](#), reinforcing its expectation that organizations provide notification whether or not such notification is legally required. Sector-specific breach notification requirements were introduced in the UK by [The Privacy and Electronic Communications \(EC Directive\) \(Amendment\) Regulations 2011](#), and since May 2011, public electronic communication service providers have been required to notify the ICO, and in some cases affected individuals, in the event of a data security breach. All other organizations are strongly encouraged to notify the ICO of serious security breaches, and the fact that an incident was reported voluntarily is something the ICO takes into consideration when determining the appropriate enforcement action. [Continue reading...](#)

Chinese Ministry of Industry and Information Technology Issues New Data Protection Regulations February 3, 2012

The Ministry of Industry and Information Technology of the People's Republic of China (the "MIIT") recently issued a regulation entitled "Several Provisions on Regulating Market Orders of Internet Information Services" (the "New Regulations"). The New Regulations, which will take effect on March 15, 2012, include significant new data protection requirements applicable to Internet information service providers ("IISPs"). Consistent with data protection regimes currently in place elsewhere in the world, IISPs will be required to provide much stronger protection for the personal data they collect from users in China, and will be subject to notice and consent requirements, collection limitations and use limitations. [Continue reading...](#)

German DPAs Comment on Proposed EU Data Protection Law Reform February 2, 2012

On January 26, 2012, the German Data Protection Commissioners ("DPAs") of the federal states Rhineland-Palatinate and Hesse held a joint [press conference](#) to present their views on the European Commission's legislative [proposal](#) for a comprehensive reform of current EU data protection rules. The day before, the European Commission [proposed](#) replacing the existing EU Data Protection Directive 95/46/EC with a [Regulation](#) that would be directly applicable in all European Member States and therefore not require implementing legislation on the national level. [Continue reading...](#)



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