

November 2014

This Client Alert is a monthly update on privacy and cybersecurity 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:

- [Massachusetts Attorney General Reaches Settlement with Boston Hospital Over Data Security Allegations](#)
- [Hunton Global Privacy Update – November 2014](#)
- [Centre's Risk Workshop II in Brussels Emphasizes that Risk-Based Approach to Privacy Does Not Change Legal Obligations but Helps Calibrate Their Effective Implementation](#)
- [Court Orders Debt Brokers to Notify Consumers Following FTC Allegations of Unlawful Disclosure of Personal Information](#)
- [TRUSTe Reaches Settlement with FTC Over Alleged FTC Act Violations](#)
- [Ebola and Other Health Emergencies Create Workplace Privacy Dilemmas](#)
- [IAPP Europe Data Protection Congress 2014](#)
- [GPEN Holds Workshop on the Use of Publicity as a Regulatory Compliance Technique](#)
- [UK ICO Issues Code of Practice Regarding the Use of Surveillance Cameras](#)
- [German Court Asks European Court of Justice if IP Addresses are Personal Data](#)
- [New Payment Technologies Should Reduce Demand for Cyber Insurance](#)
- [Federal District Court Grants Motion to Dismiss a Class Action Alleging Impermissible Sharing of Personal Information Under the Video Privacy Protection Act](#)
- ["One-Stop-Shop" Under the Proposed EU Regulation: A Way Forward](#)
- [FFIEC Announces Plans to Update Cybersecurity Guidance in Wake of Cybersecurity Assessments](#)
- [Supreme Court of Canada Extends Deadline for Amending Alberta PIPA](#)

Massachusetts Attorney General Reaches Settlement with Boston Hospital Over Data Security Allegations

November 25, 2014

On November 21, 2014, Massachusetts Attorney General Martha Coakley [announced](#) that Boston hospital Beth Israel Deaconess Medical Center ("BIDMC") has agreed to pay a total of \$100,000 to settle charges related to a data breach that affected the personal and protected health information of nearly 4,000 patients and employees. [Continue reading...](#)

Hunton Global Privacy Update – November 2014

November 21, 2014

On November 18, 2014, Hunton & Williams' [Global Privacy and Cybersecurity practice group](#) hosted the latest webcast in its [Hunton Global Privacy Update](#) series. The program covered a number of privacy and data protection topics, including a report on the [International Conference of Data Protection and Privacy Commissioners](#), highlights on the Council of the European Union's [proposed revisions](#) to the compliance obligations of data controllers and data processors included in Chapter IV of the forthcoming EU General

Data Protection Regulation, and U.S. highlights on California's breach report and Federal Communications Commission enforcement actions. [Continue reading...](#)

Centre's Risk Workshop II in Brussels Emphasizes that Risk-Based Approach to Privacy Does Not Change Legal Obligations but Helps Calibrate Their Effective Implementation November 19, 2014

On November 18, 2014, the [Centre for Information Policy Leadership](#) at Hunton & Williams (the "Centre") held the second workshop in its ongoing work on the [risk-based approach to privacy](#) and a Privacy Risk Framework. Approximately 70 [Centre members](#), privacy regulators and other privacy experts met in Brussels to discuss the benefits and challenges of the risk-based approach, operationalizing risk assessments within organizations, and employing risk analysis in enforcement. In discussing these issues, the speakers emphasized that the risk-based approach does not change the obligation to comply with privacy laws but helps with the effective calibration of privacy compliance programs. [Continue reading...](#)

Court Orders Debt Brokers to Notify Consumers Following FTC Allegations of Unlawful Disclosure of Personal Information November 17, 2014

On November 12, 2014, the Federal Trade Commission [announced](#) that in response to FTC complaints, a federal court has ordered two debt brokerage companies to notify over 70,000 consumers whose sensitive personal information was posted on a public website by the debt brokerage companies. [Continue reading...](#)

TRUSTe Reaches Settlement with FTC Over Alleged FTC Act Violations November 17, 2014

On November 17, 2014, the Federal Trade Commission [announced](#) that data privacy certifier True Ultimate Standards Everywhere, Inc. ("TRUSTe") has agreed to settle charges that the company deceived consumers about its recertification program and misrepresented that it was a non-profit entity in violation of Section 5 of the FTC Act. [Continue reading...](#)

Ebola and Other Health Emergencies Create Workplace Privacy Dilemmas November 14, 2014

Hunton & Williams [Labor & Employment](#) partner Susan Wiltsie reports:

Fears of a worldwide Ebola pandemic appear to have abated, but the tension between workplace safety and employee privacy, thrown into relief by this health emergency, remains an issue relevant to all employers. Any potential health threat created by contagious illness requires employers to plan and put into effect a reasonable response, including policies governing the terms and conditions under which employees may be required to stay away from the workplace, and in which their health care information may be relevant to workplace decisions. [Continue reading...](#)

IAPP Europe Data Protection Congress 2014 November 14, 2014

Join us at the International Association of Privacy Professionals (“IAPP”) Data Protection Congress in Brussels, November 18-20, 2014. Hunton & Williams privacy professionals will be featured speakers in the following sessions:

[Continue reading...](#)

GPEN Holds Workshop on the Use of Publicity as a Regulatory Compliance Technique November 7, 2014

On November 1, 2014, the [Global Privacy Enforcement Network](#) (“GPEN”) [posted](#) a media release on their workshop held on October 12, 2014, in Mauritius on the use of publicity as a regulatory compliance technique. The workshop, attended by 44 commissioners and staff from around the world, focused on different issues concerning privacy enforcement, including the effectiveness of monetary penalties in enforcing data protection laws and the diverse approaches to enforcement publicity. In addition, there was a public demonstration of the recently expanded World Legal Information Institute’s [International Privacy Law Library](#), which is said to be the largest freely accessible and searchable database of privacy law materials in the world. [Continue reading...](#)

UK ICO Issues Code of Practice Regarding the Use of Surveillance Cameras November 7, 2014

On October 15, 2014, the UK Information Commissioner’s Office (“ICO”) [published](#) a code of practice regarding the use of surveillance cameras (“Code of Practice”). The Code of Practice explains how the legal requirements of the Data Protection Act 1998 apply to operators of surveillance cameras. Practical and technological advancements have led to a wide variety of surveillance camera technologies that differ from traditional CCTV (e.g., Automatic Number Plate Recognition cameras and body-worn cameras). The Code of Practice addresses (1) changes in technology and (2) inconsistent standards that have arisen in various sectors since the ICO last updated its guidance on CCTV systems, which occurred in 2008. In particular, due to technological advancements, surveillance cameras are no longer merely passive recording devices, but rather can be used to identify specific items or individuals, keep detailed records of events, and are increasingly portable and discrete. [Continue reading...](#)

German Court Asks European Court of Justice if IP Addresses are Personal Data November 6, 2014

On October 28, 2014, the German Federal Court of Justice [referred](#) the question of whether an IP address constitutes personal data under the EU Data Protection Directive 95/46/EC (“EU Data Protection Directive”) to the European Court of Justice (“ECJ”). The German court referred the question to the ECJ for a preliminary ruling in connection with a case that arose in 2008 when a German citizen challenged the German federal government’s storage of the dynamic IP addresses of users on government websites. The citizen’s claim initially was rejected by the court of first instance. The claim was granted, however, by the court of second instance to the extent it referred to the storage of IP addresses after the users left the relevant government websites. Subsequently, both parties appealed the decision to the German Federal Court of Justice. [Continue reading...](#)

New Payment Technologies Should Reduce Demand for Cyber Insurance November 6, 2014

Hunton & Williams [Insurance Litigation & Counseling](#) partner [Lon Berk](#) reports:

As the demand for cyber insurance has skyrocketed, so too has the cost. One broker estimates that sales in 2014 will double from the \$1 billion premium collected in 2013. Much of the increase in demand and cost has been the result of the widely publicized hacks of the point-of-sale systems at large retailers, and the primary emphasis of most cyber policies is to address liability arising from such events. New payment technologies, however, will change the need for this type of cyber insurance. American Express recently announced a token service; Apple incorporated ApplePay into its new iPhones; and a group of retailers, the Merchant Customer Exchange, is working on the release of a new payment technology as well. These technologies, although different in detail, eliminate the need for merchants to collect unencrypted payment card information from customers, significantly reducing the risk created by point-of-sale malware. [Continue reading...](#)

Federal District Court Grants Motion to Dismiss a Class Action Alleging Impermissible Sharing of Personal Information Under the Video Privacy Protection Act November 5, 2014

On October 8, 2014, the United States District Court for the Northern District of Georgia [granted](#) Cartoon Network, Inc.'s ("Cartoon Network's") motion to dismiss a putative class action alleging that Cartoon Network's mobile app impermissibly disclosed users' personally identifiable information ("PII") to a third-party data analytics company under the Video Privacy Protection Act ("VPPA"). [Continue reading...](#)

"One-Stop-Shop" Under the Proposed EU Regulation: A Way Forward November 5, 2014

This week, the Article 29 Working Party ("Working Party") prepares to debate various proposals on the "one-stop-shop" mechanism under the proposed EU General Data Protection Regulation ("Regulation"). Hunton & Williams' [Global Privacy and Cybersecurity](#) practice and its [Centre for Information Policy Leadership](#) submitted a [strategy paper](#) on the one-stop-shop to the Working Party. The paper proposes a methodology for selecting and defining the role of a lead regulatory authority with the objective of making the one-stop-shop more operational, flexible and viable. The work draws on a more detailed article published on November 3, 2014, by Hunton & Williams senior attorney [Rosemary Jay](#) in the magazine for the Society for Computers and Law, entitled [The "One Stop Shop" – Working in Practice](#). [Continue reading...](#)

FFIEC Announces Plans to Update Cybersecurity Guidance in Wake of Cybersecurity Assessments November 4, 2014

On November 3, 2014, the [Federal Financial Institutions Examination Council](#) ("FFIEC"), on behalf of its members, [released](#) a report entitled [FFIEC Cybersecurity Assessment General Observations](#) (the "Report") that contains observations from recent cybersecurity assessments conducted at over 500 community financial institutions as part of the FFIEC cybersecurity examination work program. The Report summarizes themes from the assessments and provides suggested questions for chief executive officers and boards of directors to ask when assessing their institutions' cybersecurity preparedness. In light of the assessments, the FFIEC announced that its members will review and update current FFIEC cybersecurity guidance. [Continue reading...](#)

Supreme Court of Canada Extends Deadline for Amending Alberta PIPA November 4, 2014

On October 30, 2014, the Supreme Court of Canada [extended](#) the deadline for the province of Alberta to amend its Personal Information Protection Act ("PIPA"). In November 2013, the Supreme Court of

Canada [declared PIPA invalid](#) because it interfered with the right to freedom of expression in the labor context under Section 2(b) of the Canadian Charter of Rights and Freedoms. The Supreme Court of Canada gave the Alberta legislature 12 months to determine how to make the legislation constitutionally compliant, which it apparently failed to do. The new deadline for amending PIPA is May 2015. [Continue reading...](#)



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