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

February 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:

- SSL Bugs Likely to Have Insurance Coverage Implications
- Chairman of French Data Protection Authority Elected Chair of Article 29 Working Party
- European Data Protection Supervisor Calls for Strengthening of EU Data Protection Laws
- Greek Presidency Issues Notes on Proposed EU Data Protection Regulation
- Puerto Rico Health Insurer Reports Record Fine Following PHI Breach Incident
- Traditional Insurance Policies May Cover Cyber Risks
- German Appeals Court Finds German Data Protection Law Applicable to Facebook
- Broad Interpretations of Terrorism Exclusions Are Incompatible with Cyber Insurance
- French Data Protection Authority Revises Authorization on Whistleblowing Schemes
- FTC Announces Settlement with Online Gaming Company Falsely Claiming Compliance with the Safe Harbor Framework
- NIST Releases Final Cybersecurity Framework
- German Ministry Moves on Privacy Litigation
- European Member States and ENISA Issue SOPs to Manage Multinational Cyber Crises
- FTC Announces Settlement with Medical Transcription Provider after Discovery of Patient Transcripts on the Internet

---

SSL Bugs Likely to Have Insurance Coverage Implications
February 28, 2014

Hunton & Williams Insurance Litigation & Counseling partner Lon Berk reports:

The recently publicized Secure Sockets Layer ("SSL") bug affecting Apple Inc. products raises a question regarding insurance coverage that is likely to become increasingly relevant as "The Internet of Things" expands. Specifically, on certain devices, the code used to set SSL connections contains an extra line that causes the program to skip a critical verification step. Consequently, unless a security patch is downloaded, when these devices are used on shared wireless networks they are subject to so-called "man-in-the-middle" security attacks and other serious security risks. Assuming that sellers of such devices may be held liable for damages, there may be questions about insurance to cover the risks. Continue reading…

Chairman of French Data Protection Authority Elected Chair of Article 29 Working Party
February 27, 2014

On February 27, 2014, Chairwoman of the French Data Protection Authority (the "CNIL") Isabelle Falque-Pierrotin was elected Chairwoman of the Article 29 Working Party effective immediately. Ms. Falque-Pierrotin succeeds Jacob Kohnstamm, Chairman of the Dutch Data Protection Authority, who chaired the

Article 29 Working Party for four years. The Working Party also elected two new Vice-Chairs: Wojciech Rafal Wiewiórowski of the Polish Data Protection Authority, and Gérard Lommel of the Luxembourg Data Protection Authority. Continue reading…

European Data Protection Supervisor Calls for Strengthening of EU Data Protection Laws
February 24, 2014

On February 21, 2014, Peter Hustinx, the European Data Protection Supervisor ("EDPS"), highlighted the need to enforce existing EU data protection law and swiftly adopt EU data protection law reforms as an essential part of rebuilding trust in EU-U.S. data flows. Continue reading…

Greek Presidency Issues Notes on Proposed EU Data Protection Regulation
February 24, 2014

On January 31, 2014, the Greek Presidency of the Council of the European Union issued four notes regarding the proposed EU Data Protection Regulation. These notes, discussed below, address the following topics: (1) one-stop-shop mechanism; (2) data portability; (3) data protection impact assessments and prior checks; and (4) rules applicable to data processors. Continue reading…

Puerto Rico Health Insurer Reports Record Fine Following PHI Breach Incident
February 24, 2014

Triple-S Management Corporation reported in the 8-K it recently filed with the U.S. Securities and Exchange Commission that its health insurance subsidiary, Triple-S Salud, Inc. ("Triple S"), which is Puerto Rico's largest health insurer, will be fined $6.8 million for a data breach that occurred in September 2013. The civil monetary penalty, which is being levied by the Puerto Rico Health Insurance Administration, will be the largest fine ever imposed following a breach of protected health information. Continue reading…

Traditional Insurance Policies May Cover Cyber Risks
February 19, 2014

Hunton & Williams Insurance Litigation & Counseling partner Lon Berk reports:

Insurers often contend that traditional policies do not cover cyber risks, such as malware attacks and data breach events. They argue that these risks are not "physical risks" or "physical injury to tangible property." A recent cyber attack involving ATMs, however, calls this line of reasoning into question. Continue reading…

German Appeals Court Finds German Data Protection Law Applicable to Facebook
February 18, 2014

On January 24, 2014, the Chamber Court of Berlin rejected Facebook's appeal of an earlier judgment by the Regional Court of Berlin in cases brought by a German consumer rights organization. In particular, the court:

Continue reading…

Broad Interpretations of Terrorism Exclusions Are Incompatible with Cyber Insurance

February 14, 2014

The scale of some recent cyber events has been extraordinary. Target reports that 70 million people (almost 25% of the U.S. population) were affected by its recent breach. *CNN* recently reported that in South Korea there was a breach that affected 40% of its citizens. The staggering impact of these events is leading companies to seek protection through both technology and financial products, such as insurance. Insurers typically attempt to avoid this sort of enormous exposure with terrorism exclusions, and it is reasonable to expect aggressive insurers to rely upon such exclusions to avoid their coverage obligations. In a client alert, a Hunton & Williams Insurance Litigation & Counseling partner outlines how after 9-11, insurers added terrorism exclusions to their policies in order to provide coverage for losses arising out of terrorism only if special coverage was acquired.

Read our full client alert.

French Data Protection Authority Revises Authorization on Whistleblowing Schemes
February 14, 2014

In a decision published on February 11, 2014, the French Data Protection Authority ("CNIL") adopted several amendments to its Single Authorization AU-004 regarding the processing of personal data in the context of whistleblowing schemes (the "Single Authorization"). Continue reading…

FTC Announces Settlement with Online Gaming Company Falsely Claiming Compliance with the Safe Harbor Framework
February 13, 2014

On February 11, 2014, the Federal Trade Commission announced a proposed settlement with Fantage.com stemming from allegations that the company made statements in its privacy policy that deceptively claimed that Fantage.com was complying with the U.S.-EU Safe Harbor Framework. Continue reading…

NIST Releases Final Cybersecurity Framework
February 12, 2014

On February 12, 2014, the National Institute of Standards and Technology ("NIST") issued the final Cybersecurity Framework, as required under Section 7 of the Obama Administration's February 2013 executive order, Improving Critical Infrastructure Cybersecurity (the "Executive Order"). The Framework, which includes standards, procedures and processes for reducing cyber risks to critical infrastructure, reflects changes based on input received during a widely-attended public workshop held last November in North Carolina and comments submitted with respect to a preliminary version of the Framework that was issued in October 2013. Continue reading…

German Ministry Moves on Privacy Litigation
February 11, 2014

On February 11, 2014, Germany's Federal Minister of Justice and Consumer Protection announced that consumer rights organizations will soon be able to sue businesses directly for breaches of German data protection law. Such additional powers had already been contemplated by the German governing coalition's agreement and the Minister now expects to present a draft law in April of this year to implement them. Continue reading…

European Member States and ENISA Issue SOPs to Manage Multinational Cyber Crises
February 7, 2014

On February 5, 2014, the Member States of the EU and European Free Trade Association ("EFTA") as well as the European Network and Information Security Agency ("ENISA") issued Standard Operational Procedures ("SOPs") to provide guidance on how to manage cyber incidents that could escalate to a cyber crisis. Continue reading…

FTC Announces Settlement with Medical Transcription Provider after Discovery of Patient Transcripts on the Internet
February 3, 2014

On January 31, 2014, the Federal Trade Commission announced a settlement with GMR Transcription Services, Inc. ("GMR") stemming from allegations that GMR's failure to provide reasonable security allowed certain patients' medical transcripts to be exposed to the public on the Internet. The FTC issued an accompanying press release stating it was the FTC's 50th data security settlement. Continue reading…

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