Foreword

As we look back at 2015, one could say that data breaches was at the forefront of the public's attention throughout the year.

Multiple breaches at the U.S. government’s Office of Personnel Management led to theft of data of millions of current and former federal employees. Anthem, the second-largest health insurer in the U.S., suffered a massive attack on its IT systems and said that up to 18.8 million people could have been affected by the breach. Similarly, Premera Blue Cross also became a victim of an attack on its IT systems, and as many as 11 million persons may have been affected by the breach. The breach at Ashley Madison led to 37 million customer records being compromised. The personal information of more than 2.4 million customers of Carphone Warehouse in the UK have also been compromised. Finally, CVS and Walmart Canada have announced that a data breach at a Canadian information-technology vendor may have leaked credit card information from their online photo processing websites.

Meanwhile, the cost of data breaches is rising for companies around the world. According to a recent study conducted by the Ponemon Institute and sponsored by IBM, data breaches cost companies in the U.S. an average of $217 per compromised record, with the total average cost paid by organizations amounting to $6.5 million. And according to a recent global survey by Gemalto titled "Broken Trust: 'Tis the Season to Be Wary", 64% of consumers surveyed worldwide say “they are unlikely to shop or do business again with a company that had experienced a breach where financial information was stolen”, and 49% had the same opinion in relation to data breaches where personal information was stolen.

So as we look forward to 2016, it is likely that the protection of personal data security will be at the top of everybody’s minds – especially with the European Union’s long-awaited General Data Protection Regulation (GDPR) about to be formally adopted.

As always, please feel free to reach out to anyone in the newsletter editorial board if you have any suggestions for this newsletter. Happy New Year to everyone!
VTech data breach affects over 11 million parents and children worldwide

VTech, the manufacturer of high-tech toys for children, has announced that it suffered a security breach to its database, exposing personal data of 12 million people, including 6.4 million minors.

According to VTech's FAQ, an unauthorized party accessed VTech's customer data on their Learning Lodge app store customer database and Kid Connect servers. Since VTech directs many of its products to children under the age of 13, members of Congress have asked VTech more details on what happened, including whether the company is compliant with the Children’s Online Privacy Protection Act (COPPA) and the FTC’s COPPA regulations. COPPA generally prohibits the collection and sharing of personal information relating to children under the age of 13 without the express consent of their parents.

On December 15, 2015, it was reported that a 21-year-old man was arrested by the police in England in connection with the VTech data breach.

Suggested:

BBC News: Vtech breach: Passwords 'not securely stored'

BITS (NY Times): Man Arrested in VTech Breach of Children’s Data

Comcast to pay nearly $26 million for dumping hazardous waste and private information

On December 15, 2015, it was announced that Comcast Cable Communications had agreed to pay to the state of California $25.95 million to settle a hazardous waste disposal enforcement action that also included allegations of improper disposal of personal data.

According to the investigation, "since 2005, Comcast warehouse and dispatch facilities and customer service centers throughout the state unlawfully handled and disposed of various hazardous waste products, routinely and systematically sending these materials to local landfills that were not permitted to receive these items. The majority of the hazardous waste was electronic equipment such as remote controls, splitters, routers, modems, amplifiers, and power adapters”. It also appears that "Comcast discarded documents containing sensitive customer information, including names, addresses and phone numbers, into the trash without shredding them or making them unreadable, potentially exposing the information to identity thieves."
Press Release: Attorney General Kamala D. Harris Announces $25.95 Million Settlement with Comcast Over Hazardous Waste Disposal And Privacy Violations

San Jose Mercury News: Comcast to pay $25.95 million for dumping hazardous waste, private information

The EU's new cyber-security and privacy rules
On 7 December, the European Parliament and the European Council reached a preliminary agreement on the text of the Network and Information Security (NIS) Directive, listing minimum cyber-security requirements for operators of critical national infrastructure and digital services providers within the EU. The directive will oblige companies to ensure that their networks are robust enough to withstand cyber-attacks and to report any breach.

On 15 December, the European Commission, European Parliament, and European Council have reached political agreement on the drafting of the new EU data protection framework, the long-awaited General Data Protection Regulation (GDPR). The GDPR is expected to be adopted in early 2016 and would strengthen the EU data protection framework and streamline legislation between the 28 member states. In particular, companies operating in the EU could be subject to sanctions amounting to as much as 4% of their annual global sales if they breach the GDPR.

EU Press Release: Commission welcomes agreement to make EU online environment more secure

EU Press Release: Agreement on Commission's EU data protection reform will boost Digital Single Market

EU Fact Sheet: Data protection final agreement: Questions and answers

FTC’s $100 million settlement with LifeLock
On December 17, 2015, the FTC announced that LifeLock has settled charges and will pay $100 million to settle FTC contempt charges for violating a 2010 federal court order requiring it to secure consumers’ personal information and prohibiting it from deceptive advertising. According to the FTC's statement, this is the largest monetary award obtained by the FTC. “This settlement demonstrates the Commission’s commitment to enforcing the orders it has in place against companies, including orders requiring reasonable security for consumer data,” said FTC Chairwoman Edith Ramirez. “The fact that
consumers paid Lifelock for help in protecting their sensitive personal information makes the charges in this case particularly troubling."

On the same day, the FTC announced two more settlement agreements for COPPA violations: in the first case, LAI Systems has agreed to a $60,000 penalty for allowing third-party advertisers to collect personal information from children via persistent identifiers through apps directed to children, whereas in the second case, Retro Dreamer has agreed to pay $300,000 for allowing third parties to collect personal information from children through apps. According to the statement, one advertising network specifically warned Retro Dreamer about the obligations of the COPPA Rule and that certain of their apps appeared to be targeted to children under the age of 13.

Source:


### US Cybersecurity Information Sharing Act

On December 16, 2015, Congress passed a $1.1 trillion omnibus spending package that contained the original text of the Cybersecurity Information Sharing Act (CISA). The addition of the bill is an attempt by the federal government to incentivize companies to share indicators relating to APT attacks, breaches, phishing attacks, or malware with the ultimate goal of finding and prosecuting the perpetrators.

Many lawmakers argue that the method by which the original CISA text was added undercuts the legitimacy and importance of the legislation. By attaching the legislation to the spending package proponents guaranteed the language would pass, as a failure to do so would result in a government shutdown. Privacy groups have advocated that the language is sufficiently ambiguous such that U.S. companies are permitted to directly share user data with the NSA. They claim that the use of the word “cybersecurity” is overly broad and could permit the sharing of personally identifiable information (PII) with the NSA regardless of whether there was a nation state attack or an incident of financial fraud. Therefore, many have argued that the bill is not designed to protect users, but is instead a new method to fuel government surveillance programs.

Suggested:

Computer World: Cybersecurity bill approved, but what does it accomplish?

The Daily Dot: Congressman plans bill to repeal CISA-like legislation included in omnibus

CNBC: The controversial 'surveillance' act Obama just signed

Upcoming events
Don’t miss the upcoming programs below:

The Paris Attacks and the Data Encryption Debate

In light of the recent Paris attacks and the renewed data encryption debate, this program will examine the risks of data encryption and cyber espionage in our mobile world. What does a “backdoor” to encryption mean? Would it work? How would we protect our increasing economic dependence on the Internet with one? Didn't we have this same debate 15 years ago? This program will address these questions and more, along with a discussion of attorneys' ethical obligations of confidentiality in a world where encryption is problematic.

Format: Webinar
Date: January 7, 2016
Time: 1:00 PM - 2:30 PM ET
Credits: 1.50 General CLE Credit Hours
Panelist(s): Brendan Francis O’Connor, Richard J Johnson, Sergey Bratus
Moderator(s): Martha C Chemas

Flying on the Legal Edge with Drones: Emerging Acquisition, Security, and Regulatory Issues for Unmanned Aerial Vehicles

This program will explore the host of related legal issues, especially related to acquisition, security and regulation. International market forces and economic efficiencies will power various uses in the commercial sector. That will change how federal agencies and contractors buy and sell UAV technology.

Game-changing advances in aviation technology, guidance systems and controls have revolutionized unmanned aerial vehicles (UAV
systems or drones). For companies in the UAV business, potential cyber thefts may damage corporate IP and trade secret portfolios. They may also trigger regulatory scrutiny and enforcement risks. This program will explore the host of related legal issues, especially related to acquisition, security and regulation. International market forces and economic efficiencies will power various uses in the commercial sector. That will change how federal agencies and contractors buy and sell UAV technology.

**Format:** Webinar  
**Date:** January 12, 2016  
**Time:** 1:00 PM - 2:30 PM ET  
**Credits:** 1.50 General CLE Credit Hours  
**Panelist(s):** M Anne Swanson, Marc L Warren  
**Moderator(s):** David Z Bodenheimer

***

**National Institute on the Internet of Things**

With an estimated 75 billion connected (aka “smart”) devices to be in place by 2020, the Internet of Things (“IoT”) is potentially one of the fastest emerging, transformative, and disruptive set of technologies introduced in recent years. IoT devices are already having significant technical, social and economic impact on our connected lives. Defined with deceptive simplicity, the IoT is the interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data. These devices and sensors, which include wearables, ingestibles, systems inside moving vehicles, smart cities, home controllers and security systems, energy management, standardized and customized production environments, and mass transportation infrastructure, also bring into focus new lifespan and upgradeability issues, including security, authentication, privacy, data ownership and potential product liability on a massive scale. The disruptive growth of the IoT will require the participation of all non-consumer stakeholders (manufacturers, vendors, regulators and legislators) to address potential risks and liability. This groundbreaking conference will offer attendees an IoT deep dive, providing incisive and cutting edge insight from legal and technology experts in the field.

**Format:** In-Person  
**Location:** Jones Day, 51 Louisiana Ave NW Washington, DC 20001-2113  
**Date:** March 30-31, 2016  
**Credits:** 12.50 General CLE Credit Hours, 1.00 Ethics / Professionalism CLE Credit Hours

**Content contributors**
HJ Brehmer (hb6732a@student.american.edu) is a 1L at American University’s Washington College of Law. Prior to law school, she founded the E-Crime Investigations team at Yahoo, where she conducted a variety of criminal investigations for referral to law enforcement, domestically and internationally. These cases involved investigations of international hacking rings, large-scale account takeovers, advertising fraud, and individuals possessing and trafficking in CSAI materials. She is interested in both privacy and data security issues, primarily looking at the balance of interests between users, companies, and law enforcement. She graduated from the University of Washington, Seattle in 2012.

Kayla Gardner (kdgardner@law.bison.howard.edu) is a 2L at Howard University School of Law. She holds a Master's Degree in Criminology from GWU. She is active in the Federal Communications Bar Association, the Washington Bar Association, and the Howard Public Interest Law Society. Kayla interned last summer at the FCC in the Bureau of Public Safety and Homeland Security. She currently holds a Fall semester externship at the FCC in Commissioner Clyburn's office. She is originally from Nashville, TN, but has lived in the DC-metro area for nearly 10 years. She is interested in communications law, especially issues concerning national security and public safety such as data privacy and cybersecurity.

Paul Lanois, LL.M. (paulanocom@aol.com), is an attorney admitted to the New York Bar and the Paris (France) Bar. He regularly publishes articles on technology law and is frequently invited to speak on such topics. He was an associate at major international law firms (Simpson Thacher & Bartlett, Allen & Overy, Linklaters) and Associate Professor at the University of Cergy-Pontoise in France. He is currently senior legal counsel at an international financial institution. He graduated from the University of Paris-Sorbonne (France) with a Master's degree in Business Law and a postgraduate degree in Private and Public Economic Law. He also holds an LL.M. degree from the University of Pennsylvania Law School (USA) and the Wharton Certificate in Business and Public Policy from the Wharton School of the University of Pennsylvania. He holds the CIPP/US, CIPP/E, CIPP/C and CIPIT certifications.