Dear Readers,

Please find below the latest edition of the SciTech E-Privacy Law Committee Newsletter.

Please do not hesitate to contact us with any comments, questions, ideas or contributions you may have for this newsletter.

Paul Lanois, Nathan M. Barotz and Tamara Lev

United States: The Proposed Data Security and Breach Notification Act

As of April 2017, forty-eight states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. As news of the delay in reporting large data breaches has been frequent (e.g., Equifax, Uber), the U.S. Congress is now attempting to provide for timely nationwide notice in the event of a breach of security.

A draft bill recently introduced in the U.S. Senate entitled the "Data Security and Breach Notification Act" (the Act) would require an organization subject to Federal Trade Commission jurisdiction to notify each individual whose personal information is implicated in a data breach and to also notify credit reporting agencies if more than 5,000 people are affected. Notice would be required within 30 days of the breach unless there is justification for delay, such as a law enforcement investigation. The Act also requires regulated entities to implement information security policies and procedures similar to those required by HIPAA.

This would entail, among other things, implementing administrative, physical and technical security safeguards and the appointment of a security officer. The Act would be enforceable by both federal authorities and the state attorneys general.

Under the Act the regulated entity may be fined $1,000 per individual per day, up to $100,000 per day, for each
day that the regulated entity is out of compliance and anyone who intentionally and wilfully conceals a data breach would face up to five years in prison and fines if the breach results in $1,000 of economic harm to any individual.

Read the Proposed Bill here.

**United States: FTC Gives Final Approval to Lenovo Settlement**

The U.S. Federal Trade Commission (FTC) has given final approval to a settlement with Lenovo related to charges that the company harmed consumers by pre-loading software on some laptops that compromised security protections in order to deliver ads to consumers.

In its complaint, the FTC charged that, beginning in August 2014, Lenovo began selling consumer laptops in the United States that came with a preinstalled advertising software program called VisualDiscovery that interfered with how a user’s browser interacted with websites and created serious security vulnerabilities.

As part of the settlement with the FTC, Lenovo is prohibited from misrepresenting any features of software preloaded on laptops that will inject advertising into consumers’ Internet browsing sessions or transmit sensitive consumer information to third parties. If the company pre-installs this type of software, the order requires the company to get consumers’ affirmative consent before the software runs on their laptops. In addition, the company is required for 20 years to implement a comprehensive software security program for most consumer software preloaded on its laptops. The security program will also be subject to third-party audits.

Read the FTC announcement here.

**United States: Toymaker VTech Settles FTC Allegations That it Violated Children’s Privacy Law and the FTC Act**

Toy manufacturer VTech Electronics and its U.S. subsidiary have agreed to settle FTC charges that the company violated US privacy law by collecting personal information from children without providing direct notice and obtaining their parent’s consent and failing to take reasonable steps to secure the data it collected. VTech will pay $650,000 as part of the settlement with the FTC.

In a complaint filed by the Department of Justice on behalf of the FTC, the Commission alleges that the Kid Connect app used with some of V Tech’s electronic toys collected the personal information of hundreds of thousands of children, and that the company failed to provide direct notice to parents or obtain verifiable consent from parents concerning its information collection...
practices, as required under the Children’s Online Privacy Protection Act (COPPA). In its first children’s privacy case involving Internet-connected toys, the FTC also alleges that VTech failed to use reasonable and appropriate data security measures to protect personal information it collected.

“As connected toys become increasingly popular, it’s more important than ever that companies let parents know how their kids’ data is collected and used and that they take reasonable steps to secure that data,” said Acting FTC Chairman Maureen K. Ohlhausen. “Unfortunately, VTech fell short in both of these areas.”

The FTC also alleges that VTech violated the FTC Act by falsely stating in its privacy policy that most personal information submitted by users through the Learning Lodge and Planet VTech would be encrypted. The company, however, did not encrypt any of this information.

In addition to the monetary settlement, VTech is permanently prohibited from violating COPPA in the future and from misrepresenting its security and privacy practices as part of the proposed settlement. It also is required to implement a comprehensive data security program, which will be subject to independent audits for 20 years.

The FTC collaborated with the Office of the Privacy Commissioner of Canada, which is releasing its own Report of Findings (link is external). To facilitate cooperation with its Canadian partner, the FTC relied on key provisions of the U.S. SAFE WEB Act, which allows the FTC to share information with foreign counterparts to combat deceptive and unfair practices that cross national borders.

Read the FTC announcement here.

**United States: U.S. Customs And Border Protection Release New Rules For Searching Electronic Devices**

On January 5, 2018 U.S. Customs and Border Protection released updated guidelines for searching electronic devices. Officers of CBP, an agency of United States Department of Homeland Security, can request that people, including U.S. citizens, unlock electronic devices such as smartphones and tablets for inspection when they are entering the U.S. and officers can look through any files or applications on those devices. According to the guidelines, officers are banned from accessing cloud data which means anything that cannot be accessed while the phone’s data connection is disabled.

The guidelines also draw a distinction between “basic” and “advanced” searches. An advanced search is one where officers connect to the phone (through a wired or
wireless connection) and copy or analyze anything on it using external devices. A supervisor can approve the advanced search when there is a reasonable suspicion of illegal activity or a national security concern and "many factors" might create reasonable suspicion, including a terrorist watchlist flag or "other articulable factors."

The ACLU offered limited praise for this update. "It is positive that CBP's policy would at least require officers to have some level of suspicion before copying and using electronic methods to search a traveler's electronic device," wrote legislative counsel Neema Singh Guliani. But the group also said it "falls far short" of requiring a full search warrant. "The policy would still enable officers at the border to manually sift through a traveler's photos, emails, documents, and other information stored on a device without individualized suspicion of any kind."

In a press release, the agency reported a jump in device searches between the fiscal years of 2016 and 2017. It reportedly searched devices for .007 percent of incoming international travelers in 2017 versus .005 percent in 2016. Overall, CBP carried out 30,200 device searches in 2017, an increase over 19,051 the previous year.

Read the CBP Directive No. 3340-049A here.

**United States: Provider of cancer care services and radiation oncology agrees to pay $2.3 million to HHS' Office for Civil Rights to settle HIPAA violations**

21st Century Oncology ("21CO"), a Florida-based organization which operates 143 centers in the United States and 36 centers in Latin America, has agreed to pay $2.3 million to HHS' Office for Civil Rights to settle HIPAA violations.

Twice in 2015 after the FBI had obtained patient files that were purchased by an FBI informant, the FBI informed 21CO that patient information was obtained illegally by an unauthorized third party. 21Co conducted an internal investigation and discovered the perpetrator may have accessed its network SQL database as early as October 3, 2015. That unauthorized access impacted 2,213,597 of 21CO’s patients, including their names, Social Security numbers, insurance information, diagnoses, treatment and physicians’ names.

An investigation by OCR determined that 21CO did not conduct an accurate assessment of potential risks, failed to implement proper security measures and disclosed PHI to third party vendors without a business associate agreement.

21CO has also agreed to to implement a corrective action plan which includes completing a risk analysis and risk management plan, reevaluating its policies, educating its workforce and providing HHS OCR with all of its...
maintained business associate agreements.

21CO also recently agreed to pay the Department of Justice $26 million to settle False Claims Act allegations.

Read the HHS Press Release here.

United States: State of Wyoming Recognizes a Right to Privacy

Last month Wyoming became the 47th state to recognize a right to privacy when the Wyoming Supreme Court ruled that the state would recognize the privacy tort of intrusion upon seclusion as the law of the state.

The court had consolidated three cases in which three Wyoming state citizens claimed a violation of their privacy by the defendant Aaron’s Sales and Leasing.

The plaintiffs had claimed that the rent-to-own company had invaded their privacy by renting them laptop computers which came with software pre-installed to track physical location, monitor keystrokes, capture screenshots and remotely activate the devices’ webcams. The plaintiffs alleged that the defendant had never informed them the software was installed on their devices.

In the lower courts the defendant had successfully argued that Wyoming law did not recognize a right to privacy and therefore the plaintiffs lacked standing to sue.

In ruling that Wyoming would recognize the tort of intrusion upon seclusion, the court noted that the courts or the legislatures in 46 states have recognized a right to privacy with New York and Virginia explicitly refusing to recognize a right to privacy, while, before this decision, North Dakota and Wyoming had issued no definitive rulings on the question.

The court, in its decision, ruled that “Given our state’s policy favoring privacy interests and the legislative enactments protecting those interests, we find the tort of intrusion upon seclusion to be well adapted to our circumstances and state of society.”

The decision sends the three cases back to the Circuit Court for further proceedings.

Read the Court’s Decision here.


The Connecticut Supreme Court has held that physicians have a common law duty to keep a patient’s medical records confidential.

The plaintiff alleged that in 2005 the defendant, without
the plaintiff's permission and without warning, sent her medical file to a probate court in New Haven pursuant to a subpoena issued by an attorney for her child's father in a paternity case and that with this information the father was able to look at the plaintiff's medical file and use the highly personal information to harass, threaten and humiliate her, including filing seven lawsuits and threatening to file criminal complaints.

In 2007 the plaintiff sued the Avery Center for alleged negligence in failing to protect her medical file, infliction of emotional distress and failing to follow state and federal medical privacy laws. The trial court dismissed the suit in 2015 holding that, unlike laws in many other states, Connecticut law had yet to recognize a duty of confidentiality between doctors and their patients or that communications between patients and health care providers are privileged under common law.

In a vote of 6-0, the state’s highest court overturned the lower court.

Read the [Court's Decision here](#).

**European Union: EU’s highest court rules that exam papers are personal data**

According to the Court of Justice of the European Union (the highest court in the EU), exam candidates have the right to see their marked test papers.

The case stems from the attempts of Mr Nowak, a trainee accountant, to access his exam test paper after failing the examination for the fourth time. Mr Nowak was refused the right to see his examination script, on the ground that it did not contain personal data, within the meaning of the data protection legislation. Mr Nowak then contacted the Irish Data Protection Commissioner with a view to challenging the reason given for the refusal to disclose his examination script, however the Data Protection Commissioner replied that ‘exam scripts do not generally fall to be considered [for data protection purposes] … because this material would not generally constitute personal data’. Mr Nowak then sought legal action against that decision. Both the High Court and the Court of Appeal upheld the decision. The Supreme Court, which allowed an appeal against the judgment of the Court of Appeal, held that the action brought by Mr Nowak against the decision of the Data Protection Commissioner was admissible. However, the Supreme Court decided to stay the proceedings and to refer to the Court of Justice of the European Union for a preliminary ruling the question as to whether an examination script can constitute personal data, within the meaning of Directive 95/46.

The Court of Justice of the European Union ruled that "Article 2(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of
personal data and on the free movement of such data must be interpreted as meaning that, in circumstances such as those of the main proceedings, the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute personal data, within the meaning of that provision.” The landmark judgment could have major implications for professional bodies which administer exams.

Read the Court’s Decision here.

**European Union: Camera Surveillance of Lecture Halls Violates Professors’ Right to Privacy**

In the case of Antović and Mirković v. Montenegro the European Court of Human Rights recently held that camera surveillance of lecture halls at a Montenegro university violated the professors’ right to privacy as provided for in Article 8 of the European Convention on Human Rights (the “ECHR”). The court awarded damages to the plaintiffs of EUR 1,000 each for non-pecuniary damages and EUR 1,669.50 for costs and expenses.

In February 2011 the university installed video surveillance into the plaintiffs’ teaching auditoriums. The purpose of the surveillance cameras was to ensure the safety of property and people and to monitor teaching. Data collected from the surveillance was only accessible by the Dean of the School of Mathematics and was stored for one year.

The plaintiffs, two professors at the University of Montenegro’s School of Mathematics, brought claims for compensation against the University, the Personal Data Protection Agency (the “Agency”) and the State of Montenegro for violation of the right to a private life under Article 8 of the ECHR, specifically the unauthorized collection and processing of data on them.

The court held that Article 8 of the ECHR guarantees a right to a private life in the broadest sense which includes professional activities or activities taking place in a public context. The court restated its previous holdings that both covert and non-covert surveillance of an employee at his work place is an intrusion into his private life and that this video surveillance constituted an interference with the plaintiffs’ rights under Article 8.

The court considered whether the interference with the plaintiffs’ right to privacy had a legitimate aim and held that since there was no evidence of danger to people and property and that monitoring of teaching was not a legitimate ground for surveillance that the surveillance was a violation of the right to privacy.

Read more here.
European Union: the UK to be a 'third country' post-Brexit

According to a note published by the European Commission, the flow of personal data from countries in the European Union to the United Kingdom could be interrupted as a result of the Brexit, according to a note issued by the European Commission. The European Commission stated that unless a ratified withdrawal agreement establishes another date, all EU law will cease to apply to the United Kingdom from 30 March 2019, 00:00h (CET) and the UK would then become a “third country”. As a result, the EU rules for transfer of personal data to third Countries would apply subject to any transitional arrangement that may be contained in a possible withdrawal agreement, as of the withdrawal date.

Read the EU announcement here.

United Kingdom: 4 Firms fined for 44 million spam emails, 15 million calls and one million spam texts

The UK’s Information Commissioner’s Office announced that it has charged four companies a combined total of 600,000 GBP for their role in disturbing people with “nuisance marketing.”

Hundreds of complaints from the public about the firms prompted four ICO investigations, and resulted in the following fines:
- Barrington Claims Limited, fined £250,000 for over 15 million automated calls,
- Newday Limited fined £230,000 for over 44 million spam emails,
- Goody Market UK Limited fined £40,000 for 111,367 spam texts and
- TFLI Limited fined £80,000 for over 1.19 million spam texts.

Andy Curry, ICO Enforcement Group Manager, said:
“Firms cannot get away with failing to follow the rules designed to protect people from the irritation and, on occasions, distress nuisance calls, emails and texts cause.”

Read the ICO announcement here.

Australia : Reminder - New Mandatory Data Breach Laws Applicable from 22 February 2018

From 22 February 2018, all entities covered by the Australian Privacy Principles (APPs) will have clear obligations to report eligible data breaches. Entities will be required to take all reasonable steps to ensure an assessment is completed within 30 days. If an eligible data breach is confirmed, as soon as practicable they
must provide a statement to each of the individuals whose data was breached or who are at risk, including details of the breach and recommendations of the steps individuals should take. A copy of the statement must also be provided to the Office of the Australian Information Commissioner (OAIC).

Read more about the Notifiable Data Breaches scheme.

**China: Local Tech Firms Summoned By Chinese Government Over User Privacy Issues**

China’s Ministry of Industry and Information Technology (MIIT) has summoned three of the country’s leading technology firms to answer questions as they have failed to fully disclose the collection of personal data from users, reports Reuters. The regulator said Ant Financial (a payment affiliate of Alibaba Group Holding Ltd), search engine giant Baidu as well as Beijing Bytedance Technology (which oversees popular news aggregation app Jinri Toutiao) had “inadequate” policies relating to personal information protection and that any violations would be investigated and “severely punished.”

Although MIIT did not set out any specific punishments at this stage, it said the companies will conduct a review to improve product design and internal management practices.

Ant Financial’s Alipay was recently criticised by regulators after users discovered that a feature detailing spending statistics automatically enrolled them into the company’s credit rating programme, giving Alipay access to a wide array of user data. Ant Financial has since suspended the program and says it is conducting an internal review. In addition, a government-backed consumer protection group said it is suing Baidu in the eastern province of Jiangsu for failing to properly notify users about which data it is collecting. According to the lawsuit, Baidu’s search app and mobile browser fail to inform consumers that the apps enable Baidu to monitor the user’s phone and have access to messages, contacts and system settings. Earlier this week, Tencent Holdings, whose WeChat messaging app has more than 1 billion users worldwide, denied storing any user chat histories, after Chinese automotive industry tycoon Li Shufu reportedly slammed the company for invading user privacy – another sign that privacy worries increase among Chinese internet users.

Read the Press release from China’s Ministry of Industry and Information Technology here (in Chinese).

**Other privacy related news**

In the first days of 2018, published research revealed that nearly every computer chip manufactured in the last 20 years contains fundamental security flaws, with specific
variations on those flaws being dubbed Spectre and Meltdown. The flaws arise from features built into chips that help them run faster, and while software patches are available, they may have impacts on system performance. There is as of yet no evidence that these flaws have been exploited in the wild, but such exploits would be difficult to detect, and the flaws are so fundamental and widespread that security researchers are calling them catastrophic. Read more: Spectre and Meltdown explained: What they are, how they work, what’s at risk

In one last effort to convince the Supreme Court to hear its data breach case, attorneys with CareFirst warned that without the high court’s review, companies in any industry would be inundated with class-action lawsuits. CareFirst is asking the Supreme Court to review an August decision by the U.S. Court of Appeals in the District of Columbia, which ruled the risk of injury from a 2014 data breach was substantial enough for CareFirst members to move forward with their lawsuit. In a final reply brief (PDF), attorneys for the insurer argued that if that decision stands, any individual whose information was exposed in a data breach could sue the company “even if the plaintiff suffered no harm whatsoever.” Read more: In a final appeal to the Supreme Court, CareFirst warns of a ‘flood’ of data breach lawsuits

Future events

Preparing Your Vendor Agreements for the General Data Protection Regulation

Date: January 31, 2018
Time: 11:00 AM - 12:00 PM CT

Whether based in or outside the European Union, organizations that process the personal data of individuals located in the EU must prepare to comply with the General Data Protection Regulation ("GDPR")—a tougher and more complicated regulatory framework.

Replacing the 1995 Data Protection Directive, the GDPR tightens restrictions on the collection and use of personal data and permits national data protection authorities to impose fines of up to the greater of four percent of an organization’s annual global revenue or €20,000,000 for each infringement.

Starting May 25, 2018, organizations that process personal data in the context of their European operations, offer goods or services to the EU, or track the behavior of individuals located in EU must comply with the new law. Updating their vendor agreements to comply with the GDPR is one of the changes that organizations must make.

Please join Mayer Brown partners Oliver Yaros, Lei Shen, and Joseph Pennell as they discuss the GDPR and how
to update these agreements. They'll cover topics including:

What the new requirements under the GDPR are
Overview of recent guidance provided by the Article 29 Working Party and DPAs
What companies can expect—immediately and down the road—with the GDPR implementation
How companies can best prepare to meet the obligations introduced by and avoid the substantially tougher sanctions under this new law
How companies should be updating their vendor agreements to comply with the GDPR

Read more [here](#).

**Internet of Things National Institute**

**Format:** In-Person  
**Location:** Crowell & Moring LLP, 1001 Pennsylvania Ave NW Washington, DC 20004-2543  
**Date:** May 9-10, 2018  
**Credits:** 12.75 General CLE Credit Hours

The Internet of Things (IOT) is defined as billions of vehicles, buildings, process control devices, wearables, medical devices, drones, consumer/business products, mobile phones, tablets, and other “smart” objects that are wirelessly connecting to and communicating with each other. This new top law practice area is raising unprecedented legal and liability issues.

As one of the most transformative and fast-paced technology developments in recent years, IoT will require businesses, policymakers, and lawyers (M&A, IP, competition, litigation, health law, IT/outsourcing, and privacy/cybersecurity) to identify and address the escalating legal risks of doing business in a connected world. Attend this institute to:

Discover why corporate, law firm, government, university, and other attendees gave the last two IoT Institutes rave reviews, calling it “magical,” “eye-opening,” with “rock star” speakers, and overall “a grand slam.”

Gain insights and practical guidance on the latest legal, legislative, regulatory, and liability issues of the IoT transformation—a game-changer for businesses, policymakers, and lawyers that’s generating hundreds of billions of dollars in spending globally.

Explore need-to-know IoT hot topics: big data/privacy, cybersecurity, litigation/mitigation, cloud/artificial intelligence, connected healthcare, ethics, global IoT product development and sales, insurance risk allocation, and homeland/national security.

Read more [here](#).
Editors

Paul Lanois - Mr Lanois is a global privacy, data protection and information security professional and is an attorney admitted to the Bars of the District of Columbia (DC-USA), New York (NY-USA) and the Supreme Court of the United States (SCOTUS). He regularly publishes articles on technology law and is frequently invited to speak on such topics. He has spoken at conferences across Europe, Asia and the United States. He was named a "Cybersecurity & Data Privacy Trailblazer" by the National Law Journal and an "Innovative Corporate Counsel" by Law 360. He was also recognized as a leading lawyer in The Legal 500’s GC Powerlist. He has been recognized as a Fellow of Information Privacy (FIP) by the International Association of Privacy Professionals (IAPP) and is a Certified Information Privacy Professional, with concentrations in Asian law (CIPP/A), US law (CIPP/US), European law (CIPP/E) and Canadian law (CIPP/C). He is also a Certified Information Privacy Manager (CIPM) and a Certified Information Privacy Technologist (CIPT). He was an Associate Professor at the University of Cergy-Pontoise in France and an associate at major international law firms (Simpson Thacher & Bartlett, Allen & Overy and Linklaters). 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 a Certificate in Business and Public Policy from the Wharton School at the University of Pennsylvania.

Nathan M. Barotz - Mr. Barotz has been in the private practice of law for over 25 years. A graduate of Duke University (cum laude) and the George Washington University Law School, Mr. Barotz originally developed a focus on health care law which in the last ten years has led to his strong interest the rapidly developing body of law governing IoT, cybersecurity and privacy. For the last five years, Mr. Barotz has served in the role of general counsel and compliance and privacy officer for companies utilizing telemedicine technology in post-acute patient treatment and currently serves in that role for HomeSleep, LLC, a company which specializes in diagnostic testing for sleep apnea. Mr. Barotz is a member of the New York State and Connecticut State Bars, the United States District Court Bars, Southern District and Eastern District of New York and has received his CIPP/US certification from the International Association of Privacy Professionals.

Tamara Lev - Ms. Lev is a consultant specializing in data privacy, information security, and regulatory compliance. She assists her clients with diligence and care, while identifying potential privacy vulnerabilities and conducting information security risk assessments. Tamara is a law graduate from Ono Academic College with a LLB in Law. She is a Fordham Law School graduate with a
LLM in Intellectual Property and Information Technology.
Tamara is a member of the State Bar of New York.