Skadden

# Privacy & Cybersecurity Update



## Eleventh Circuit Vacates Order Against LabMD, Dealing Significant Blow to FTC Orders That Require Reasonable Security Procedures

**An Eleventh Circuit decision has held that the Federal Trade Commission (FTC or commission) cease-and-desist orders that require companies to implement "reasonable security procedures" are too vague to be enforceable.**

On June 6, 2018, the U.S. Court of Appeals for the Eleventh Circuit vacated the cease-and-desist order that the Federal Trade Commission had issued to LabMD for failure to maintain "reasonable and appropriate security for personal information on its computer networks." Although the court did not shed any light on whether the failure to provide "adequate" data protection measures could constitute an "unfair act or practice" under Section 5 of the Federal Trade Commission Act, the court did reject the concept that an FTC order could require a company to adopt "reasonable security requirements," thereby striking a significant blow to the FTC's approach to cybersecurity issues.

### Background

LabMD, a now-defunct medical laboratory, relied on medical specimen and patient information to recommend diagnoses to doctors. Due to the nature of the information required for operation, it employed a data security program and was subject to regulations issued under the Health Insurance Portability and Accountability Act (HIPAA). In 2005, LabMD's billing manager downloaded the peer-to-peer file-sharing application Limewire onto her work computer, which accidentally exposed a 1,718-page file (the 1718 File) containing the personal information of 9,300 consumers to other Limewire users. There was no evidence any Limewire user ever accessed the file. Rather, a data security firm found the file and tried to sell LabMD its security services. When LabMD declined, the security firm handed the 1718 File to the FTC.

The FTC issued an administrative complaint against LabMD, alleging that it had committed an "unfair act or practice" prohibited by Section 5 of the FTC Act. Rather than specifying

any improper activity in which LabMD had engaged, the complaint listed seven broad data security measures that LabMD failed to perform. LabMD filed a motion to dismiss for failure to state a claim, which was denied by the commission. LabMD's subsequent motion for summary judgment also was denied by the agency.

At the subsequent evidentiary hearing, an administrative law judge (ALJ) dismissed the complaint in favor of LabMD, stating that the FTC had not proven that there was substantial injury or a likelihood of substantial injury to consumers, a required showing for allegations of "unfair act or practice" under Section 5. The FTC appealed the ALJ's decision to the full commission for review which, unsurprisingly, reversed the ALJ's decision, finding that LabMD's failure "to implement reasonable security measures to protect the sensitive consumer information on its computer network" rendered its data security practices "unfair under Section 5." The commission entered an order enjoining LabMD to update its data security protection to a proficiency that meets the FTC's reasonableness standard. LabMD then appealed to the Eleventh Circuit.

### The Eleventh Circuit Decision

The Eleventh Circuit was presented with two issues: (1) whether a failure to provide "adequate" data protection measures could constitute an "unfair act or practice" under Section 5 and (2) whether the cease-and-desist requiring LabMD to comply with extensive and broad remedial measures identified in the order was enforceable. In acknowledging that the commission must rely on "clear and well-established" policies that are expressed in the Constitution, statutes or the common law when enforcing its unfairness standards, the court pointed to the common law of negligence to "assume *arguendo* that the Commission is correct and that LabMD's negligent failure to design and maintain a reasonable data-security program invaded consumers' right of privacy and thus constituted an unfair act or practice." Essentially, the court declined to decide whether negligence or a failure to provide "adequate" data protection measures can constitute an "unfair act or practice" under Section 5 — it merely assumed that the FTC has that authority.

Turning to the second issue, the court found the FTC's cease-and-desist order to be unenforceable due to a lack of specificity, with the court adopting a novel approach to analyzing this issue. The court noted that, as a general matter, if the FTC believes a defendant is violating such an order, the court could move for an order requiring the defendant to show cause outlining why it should not be held in contempt for engaging in conduct the order specifically enjoined. If the defendant is unable to do so, the court may adjudicate the defendant in civil contempt and impose sanctions. The Eleventh Circuit noted that this approach is untenable where the cease-and-desist order does not contain any specific prohibitions that can be violated (or not), and instead imposes a vague requirement that LabMD engage in a series of preventative measures to elevate its data security program to an "indeterminable standard of reasonableness."

The court proceeded to posit out a scenario to prove its point:

- Assume the FTC alleges that LabMD failed to implement step "x" and therefore its security program was not "reasonably designed." LabMD's expert says "x" is not required, but the FTC expert says it is required. Since the order did not specify "x," the court would have to always reject the FTC's argument since if it imposed "x" as a new requirement, it would be modifying a cease-and-desist order which is not permitted at a show cause hearing. The court further reasoned that if the FTC kept coming up with new requirements that LabMD had to satisfy to prove a well-established security program, the district court would end up "managing LabMD's business in accordance with the Commission's wishes" and decided that this "micromanaging is beyond the scope of court oversight contemplated by injunction law."

### Key Takeaways

The Eleventh Circuit did not weigh in on whether the FTC has the authority to enforce cybersecurity measures, instead it merely assumed that the commission has that right on a theory of common law negligence, an argument that the commission did not itself make. Had the court undermined the FTC's authority, it would have directly contradicted the Third Circuit's decision in *FTC v. Wyndham Worldwide Corp.*, which explicitly stated that the FTC has authority to regulate data security.

However, the Eleventh Circuit decision went to the heart of many FTC cease-and-desist orders in the cybersecurity area. In many of these cases, the FTC has not alleged that the defendant engaged in a specific improper activity, rather it has made sweeping pronouncements that the defendant did not have reasonable cybersecurity measures in place, and then required cease-and-desist orders imposing this vague standard. The Eleventh Circuit decision suggests that such vague orders will no longer be enforceable. The court's well-reasoned analysis as to how such a cease-and-desist order would play out in an order-to–show-cause hearing will make it difficult for other courts to limit the decision to the specific facts of LabMD. Companies will undoubtedly challenge any consent decrees and/or equitable orders that contain vague cybersecurity standards.

Return to Table of Contents

## Colorado, Louisiana and Vermont Strengthen Data Breach Notification Laws

**In line with recent national trends, three states have increased requirements for data breach notifications.**

### Colorado

On May 29, 2018, the state of Colorado enacted a bill requiring entities that experience a data breach to provide notice to affected individuals within 30 days of determining that a breach has occurred. This will be the shortest notification time period of any state's data breach law as of when the law goes into effect on September 1, 2018.

Every state has a data breach notification statute that requires notice to individuals who have been affected by data breaches involving personally identifiable information. However, each state's law sets out different notice requirements, including when the entity must notify the affected individuals. Many of these laws contain vague timing standards — which have thus far been interpreted loosely — and do not expressly specify how quickly entities have to provide notice. As we reported in our March 2018 *Privacy & Cybersecurity Update*,[1] there has been a trend toward defining timing standards in data breach notification laws, with the last two states to enact data breach notification standards, South Dakota and Alabama, each including notice requirements (60 days and 45 days respectively) in their regulations.

Colorado's new statute will have the shortest time period without any exemption for the notification requirement. Although Florida's data breach notification statute also contains a 30-day requirement, it provides entities a 15-day extension if there is "good cause for delay." Given the national nature of most data breaches, compliance with Colorado law will set the bar for data breach notifications nationwide.

The law also imposes new requirements regarding the content of notifications. While some state laws do not address the information required to be disclosed, Colorado joined several other states that require the inclusion of data, including the date of the breach, a description of the personally identifiable information exposed and contact information for the entity. Colorado also will require notices to include toll-free numbers, addresses and websites for consumer reporting agencies and the FTC in addition to a statement that Colorado residents can obtain information from the FTC and credit reporting agencies about fraud alerts and security breaches.

Effectively, the law also reduces the time allowed to provide notification for breaches of medical information by half. Under the HIPAA Breach Notification Rule, entities have 60 days after a breach to notify affected individuals. Personal information under the new Colorado law will include medical information and health insurance identification numbers, which means the state law will effectively override the HIPAA 60-day window.

### Louisiana

Effective August 1, 2018, an amendment to Louisiana's Database Security Breach Notification Law will require entities to provide notice within 60 days of discovering a breach. This also applies to third parties that are required to notify the owners of the personal information in the event of a breach. The law allows for reasonable extensions to be determined by the state attorney general if required by law enforcement or if more time is necessary to determine the scope of the breach, prevent further disclosure and/or restore the integrity of the system.

In addition to imposing a timeframe for notice, the law also reduces the requirements for substitute notifications. An e-mail notification, conspicuous posting on the entity's website or notification through major statewide media is allowed when the cost of providing notifications would exceed $100,000 or the affected class is greater than 100,000 people (formerly $250,000 and 500,000, respectively). Substitute notifications also are still available if the entity is unable to obtain sufficient contact information.

Louisiana also will now require anyone who owns or licenses computerized data, including personal information, to maintain reasonable security procedures to prevent unauthorized disclosure and to take reasonable steps to destroy records containing personal information that no longer needs to be retained.

### Vermont

Vermont recently became the first state to enact legislation to regulate data brokers. A data broker is defined as a business that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship. Data brokers are now required to make annual disclosures to the state attorney general detailing the number of data breaches and affected consumers per year.

### Key Takeaways

The three states' new laws all fall in line with recent legislation enacted throughout the country. Each of these laws require various disclosures timing requirements that companies must learn to comply with, signaling an increased focus across America

[1] Please see our March 2018 Privacy & Cybersecurity Update.

on the importance of timely notification and reporting to ensure consumers' personal information.

Return to Table of Contents

## Civil Liberties Committee Criticizes Effectiveness of the EU-US Privacy Shield

**The European Parliament's Committee on Civil Liberties (the Committee) outlined its concerns about the EU-U.S. Privacy Shield, arguing that recent data breach cases show its ineffectiveness and echoing criticisms of the Safe Harbor.**

On June 12, 2018, the European Parliament's Committee on Civil Liberties called on the European Commission to suspend data transfers that rely on the EU-U.S. Privacy Shield unless the U.S. fully complies with the framework's requirements by September 1, 2018. The Committee highlighted the disclosure of Cambridge Analytica's use of Facebook data and the recently enacted Clarifying Lawful Overseas Use of Data (CLOUD) Act in the U.S. to support their argument that the Privacy Shield fails to provide sufficient data protection for EU citizens.

### Background

In 2016, the United States and the European Commission adopted the EU-U.S. Privacy Shield, a self-certification program designed to enable U.S. companies to take in transfers of personal data from the EU and the three European Economic Area member states — Norway, Liechtenstein and Iceland — to the U.S. Under the Privacy Shield, companies self-certify their adherence to seven broad data privacy principles. Although enacted when the EU Data Protection Directive was in effect, the Privacy Shield still applies under the General Data Protection Resolution.

The Privacy Shield replaced the previous data sharing structure between the EU and U.S. known as the Safe Harbor Privacy Principles, which the Court of Justice of the European Union invalidated in October 2015 in *Schrems v. Data Protection* Commissioner. In the *Schrems* decision, the court found that the Safe Harbor failed to adequately protect the privacy of EU citizens, mainly due to the U.S. government's ability to access personal data for national security purposes. The Privacy Shield aimed to remedy the perceived inadequacies of the Safe Harbor by imposing certain restrictions on the collection of EU personal data by the U.S. government and appointing an ombudsman to oversee such collection practices. After the Privacy Shield's adoption, many privacy advocates criticized the replacement framework for failing to address the governmental surveillance concerns raised in *Schrems*.[2]

### Civil Liberties Committee's Argument

The Committee pointed to the Cambridge Analytica's use of Facebook data, which resulted in the disclosure of 87 million users' personal data to third parties in 2014, to demonstrate the ineffectiveness of the Privacy Shield. Particularly, the Committee noted that although this disclosure occurred before the Privacy Shield was in place, both Facebook and Cambridge Analytica's affiliate company, SCL Elections, are listed on the Privacy Shield register. Committee members emphasized a greater need for monitoring under the agreement and recommended that companies that misuse data be promptly removed from the Privacy Shield.

### The CLOUD Act

In addition, the Committee voiced concern about the United States' recent adoption of the CLOUD Act, which grants U.S. and foreign police services access to personal data across borders. The Committee indicated that this new U.S. law could be in direct conflict with EU data protection laws and have serious implications for EU citizens.

The CLOUD Act, which was passed as part of the omnibus government spending bill in March 2018, allows federal law enforcement to compel U.S.-based technology companies, via warrant or subpoena, to provide requested data stored on servers, regardless of where those servers are located. The act also allows the president to enter into executive agreements with foreign governments to provide direct access to personal data stored in the United States. The initial agreements are not subject to review by any court and need only be certified by the executive branch. Congress can object to the agreements, but does not have an approval or veto right.

Proponents of the CLOUD Act assert that the act allows national law enforcement to be more nimble and effective because the bureaucracy surrounding access to data necessary for their investigations has been substantially lessened.

The Committee argued that the Cloud Act provides a loophole to the Privacy Shield and the Schrems decision, violating EU citizens' data privacy rights. In essence, the Committee contended that the act weakens the Privacy Shield and resurfaces the concerns that led to replacing the Safe Harbor in the first place.

While privacy advocates have expressed concerns about the provision, the act includes at least one safeguard to protect

[2] For more information regarding criticism of the Privacy Shield, see our April 2017 Privacy and Cybersecurity Update.

personal data. A provider can file a motion to quash when it "reasonably believes" the "customer or subscriber is not a United States person and does not reside in the United States"[3] and there is a "material risk" that production of the compelled data would violate the laws of a "qualifying foreign government." This precaution, however, can only be exercised by a provider, not by an individual whose personal data is at risk of disclosure.

### Key Takeaways

Many pundits have questioned whether the Privacy Shield would come under the same attacks that had been leveled against the Safe Harbor. The statement of the Committee suggests that this will indeed be the case.

Return to Table of Contents

## AIG Reports Increase in Cyber Insurance Purchases and Claims

**A recent report by insurance carrier AIG Europe (report),[4] which is based on an analysis of hundreds of insurance claims noticed under AIG cyber insurance policies, signaled an increase in cyber insurance purchases by companies while also highlighting a marked increase in cyber-related claims, underscoring the trend that businesses of all types continue to be targeted by cyber criminals.**

A recent report by insurance carrier AIG Europe (report), which is based on an analysis of hundreds of insurance claims noticed under AIG cyber insurance policies, signaled an increase in cyber insurance purchases by companies while also highlighting a marked increase in cyber-related claims, underscoring the trend that businesses of all types continue to be targeted by cyber criminals.

The recently released AIG report reinforces that businesses are taking steps to protect themselves by increasingly purchasing cyber insurance while also reporting cyberattacks under their policies when they occur to mitigate the severity of cyber-related loss.

The report outlines clear growth in cyber claims frequency, reporting that the company had as many cyber-related claims notifications in 2017 as it did in the previous four years combined, representing what AIG posits is a reflection of "a broader trend of cyber loss escalation." In a similar vein, AIG also reported that the purchase of cyber insurance has significantly increased in the wake of recent large-scale ransomware and denial-of-service attacks, which AIG predicts is likely to contribute to even greater claims frequency going forward. "We're seeing a lot more interest now from nontraditional buyers of cyber insurance, so [we] can expect an increase year-over-year in the number of claims, just based on the growth of the premium," AIG stated in the report.

According to claim statistics in the report, ransomware is the top cause of cyber loss, accounting for 26 percent of reported cyber claims, followed by hacker data breaches (12 percent), other security failure/unauthorized access (11 percent) and impersonation fraud (9 percent). While cyber loss caused by employee negligence (*e.g.*, inadvertent release of personally identifiable information) accounted for only 7 percent of claims, AIG reports that "human error continues to be a significant factor in the majority of cyber claims."

AIG's claims statistics further illustrate that no industry sector is immune to cyberattacks. Indeed, according to the report, there is "a continuing trend, whereby a larger number of notifications each year are coming from an increasingly broader range of industry sectors . . . not just those traditionally associated with cyber risk." In 2017 alone, for example, AIG received cyber claim notifications from eight sectors that had never reported any cyberattacks to AIG in previous years.

Although it does not specify the eight sectors with new cyber claims experience, the report states that AIG saw the greatest number of cyber claims in 2017 from businesses in the financial and professional services industries, accounting for 36 percent of claims. Notably, although at the top of the list, the financial services industry, a sector commonly associated with cyber risk, actually saw a decrease in claims frequency (18 percent down from 23 percent in 2013-16). By contrast, the professional services industry, a sector not as commonly associated with cyber risk, saw an increase in claims frequency (18 percent up from 6 percent in 2013-16). Tailing the financial and professional services industries in claims frequency was the retail/wholesale industry (12 percent), the business services industry (10 percent) and the manufacturing industry (10 percent).

### Key Takeaways

As the report demonstrates, cyber criminals are more frequently relying on innovative techniques, such as ransomware, and are striking across industry borders. As the frequency, severity and sophistication of cyberattacks continue to escalate, the upward trends reported by AIG are likely to continue as more and more companies consider cyber insurance as one component of a comprehensive risk management plan.

Return to Table of Contents

[3] 18 U.S.C. § 2713 (h)(2).

[4] The report, *Cyber Insurance Claims: Ransomware Disrupts Business*, can be accessed here.

## Contacts in the Cybersecurity and Privacy Group

**Stuart D. Levi**
Partner / New York
212.735.2750
stuart.levi@skadden.com

**James Carroll**
Partner / Boston
617.573.4801
james.carroll@skadden.com

**Brian Duwe**
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

**David Eisman**
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

**Patrick Fitzgerald**
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

**Todd E. Freed**
Partner / New York
212.735.3714
todd.freed@skadden.com

**Marc S. Gerber**
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

**Lisa Gilford**
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

**Rich Grossman**
Partner / New York
212.735.2116
richard.grossman@skadden.com

**Michael E. Leiter**
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

**Amy Park**
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

**William Ridgway**
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

**Ivan Schlager**
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

**David Schwartz**
Partner / New York
212.735.2473
david.schwartz@skadden.com

**Jen Spaziano**
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

**Donald L. Vieira**
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

**Helena Derbyshire**
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

**Jessica N. Cohen**
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

**Peter Luneau**
Counsel / New York
212.735.2917
peter.luneau@skadden.com

**James S. Talbot**
Counsel / New York
212.735.4133
james.talbot@skadden.com



Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000