Skadden

# Privacy & Cybersecurity Update



## US Supreme Court Holds That Consumer Plaintiffs Must Show 'Real Harm' to Sue in Federal Court

**In *Spokeo*, the U.S. Supreme Court held that a consumer class action plaintiff could not sue a company for mere technical violations of the Fair Credit Reporting Act. To have standing to sue, the plaintiff must demonstrate actual injury.**

On May 16, 2016, the U.S. Supreme Court vacated and remanded the U.S. Court of Appeals for the 9th Circuit's decision in *Spokeo, Inc. v. Thomas Robins*, holding that the circuit court used an "incomplete" analysis when it ruled that consumers can sue companies without alleging actual injury. In determining whether a plaintiff has standing to sue for statutory violations, a court must address both aspects of the injury-in-fact standing requirement — namely, whether the plaintiff suffered an injury that is both particularized and concrete.

### Background and Claim

Spokeo is a "people search engine" that, in response to user-generated requests, searches a wide array of sources to collect and report information about an individual, such as address, phone number, marital status, age, occupation, hobbies and finances. In 2011, Thomas Robins sued Spokeo in a putative class action after discovering that his Spokeo profile stated he was married with children, in his 50s, relatively wealthy, and that he had a graduate degree and a job — all of which Robins asserted was inaccurate. Robins alleged that Spokeo willfully failed to comply with the Fair Credit Reporting Act's (FCRA) requirement that consumer reporting agencies follow reasonable procedures to assure maximum possible accuracy of consumer reports.

### Lower Court Decisions

The district court dismissed Robins' suit, holding that he had not pleaded an injury-in-fact necessary to establish standing under Article III. The 9th Circuit reversed, stating that "the violation of a statutory right is usually a sufficient injury in fact to confer standing." The 9th Circuit held that Robins' complaint satisfied the injury-in-fact

requirement because (1) Robins alleged that "Spokeo violated *his* statutory rights, not just the statutory rights of other people," and (2) Robins' "personal interests in the handling of his credit information are individualized rather than collective."

### Supreme Court Decision

In a 6-2 decision, the Supreme Court reversed the 9th Circuit. In considering whether consumers can sue companies for statutory violations in the absence of actual injury, the Court instructed that the injury-in-fact requirement for standing under Article III requires a plaintiff to demonstrate an injury that is both particularized and concrete. The Supreme Court held that the 9th Circuit's analysis was "incomplete" because both of the court's conclusions about Robins' alleged injury concerned particularization, not concreteness. While particularization requires the injury to affect the plaintiff in a personal and individual way, concreteness requires the injury to actually exist — to be real, not abstract. Thus, the Supreme Court held, "Robins could not ... allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."

The Supreme Court acknowledged that "concrete" is not necessarily synonymous with "tangible" and that in some cases, Congress and the Court have recognized certain intangible harms (such as in the First Amendment context) as injuries in fact. The Court cautioned, however, that this does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a right and purports to authorize that person to sue to vindicate that right. Rather, "Article III standing requires a concrete injury even in the context of a statutory violation." With respect to the FCRA, the Supreme Court noted that a violation may result in no injury, because not all inaccuracies cause harm or present a material risk of harm. Concluding that the 9th Circuit failed to consider both the particularization and concreteness prongs of injury-in-fact analysis, the Supreme Court remanded the case to the 9th Circuit.

### Key Takeaway

The *Spokeo* decision has been hailed as a win by businesses and consumer advocates alike. Businesses facing "no-injury" class actions — those in which the alleged "injury" is simply a violation of a statute or regulation without an actual or imminent harm — have embraced the decision, expecting it will make it easier for defendants to have such actions dismissed. Consumer advocates have claimed *Spokeo* as a victory, commenting that the decision does not eliminate the ability to establish Article III standing for intangible harms or a material risk of harm; it merely clarifies the need to consider both concreteness and particularization. While the full impact of *Spokeo* remains to be seen, federal appellate courts have already begun to remand cases with instructions to consider both aspects of the injury-in-fact analysis, and defendants have begun using *Spokeo* in their defense of class actions. Companies facing claims in federal court for alleged statutory violations should scrutinize the complaints to determine whether there is a basis for challenging standing due to lack of a particularized and concrete harm.

Return to Table of Contents

## Maryland Court Dismisses Data Breach Class Action Based on Speculative Harm

**In *Chambliss v. CareFirst, Inc.*, a Maryland federal court held that a data breach class action could not proceed because the named plaintiffs failed to allege an actual injury-in-fact and thus lacked standing to sue.**

On May 27, 2016, a Maryland district court dismissed a putative class action brought by CareFirst policyholders affected by data breaches, holding that the plaintiffs lacked standing because the complaint did not allege facts showing "certainly impending" harm or a "substantial risk that the harm will occur" as a result of the breaches.[1] This decision underscores that where information is compromised as a result of a data breach, speculative harm will not suffice; to have standing, the plaintiffs must point to actual injury or a significant risk of actual, impending injury.

### Background and Claim

CareFirst, Inc. is a health insurance provider operating in Maryland, Virginia, and the District of Columbia. In 2014 and 2015, CareFirst suffered two data breaches. Both breaches affected subscribers' personal information, such as names, birth dates, email addresses and subscriber identification numbers. CareFirst denied that any confidential medical records were implicated in either breach.

In response to the breaches, two policyholders filed a putative class action, asserting claims for negligence, breach of implied contract, unjust enrichment and declaratory judgment. The plaintiffs alleged that CareFirst should have known earlier about both breaches, and that due to CareFirst's failure to adequately secure subscribers' personal information, members of the putative class faced an increased risk that unknown hackers would use that information for fraudulent charges and other forms of identity theft. The plaintiffs did not point to any actual identity theft or fraudulent charges but asserted four forms of injury: (1) an increased risk of identity theft, (2) mitigation costs incurred, (3) benefit of the bargain loss, and (4) decreased value of personal information.

[1] *Chambliss et al. v. CareFirst, Inc. et al.*, case number 1:15-cv-02288, in the U.S. District Court for the District of Maryland.

### The Court's Decision

The Maryland district court dismissed the plaintiffs' claims. The court held that the plaintiffs did not have Article III standing because none of their theories of injury rose to the level of an injury-in-fact.

Rejecting each of the plaintiffs' theories of damages in turn, the court agreed with CareFirst that any increased risk of identity theft was too speculative to support a claim. The court distinguished *CareFirst* from other data breach cases involving information more easily used in fraudulent transactions (such as credit card information) and cases where hackers had already misused the stolen data in such a way that the risk of future harm was "certainly impending" (*i.e.*, where stolen data had already been circulated online or used to make fraudulent purchases). Because there was no "certainly impending" harm in CareFirst, the court also held that any mitigation costs of purchasing credit monitoring services could not establish an injury-in-fact.

The court rejected the plaintiffs' other assertions of injury (that they suffered a loss of benefit-of-the-bargain or that they suffered a decreased value of personal information) because the complaint failed to allege facts supporting either of those theories.

### Key Takeaway

Standing continues to be a major obstacle to class actions arising from data breaches. The *CareFirst* decision highlights that injury-in-fact can be particularly difficult to establish where plaintiffs allege future, speculative harm as the basis for their claims. Companies facing putative class actions based on allegations of future harm should carefully analyze complaints to determine whether plaintiffs have alleged facts to show that the future harm is "certainly impending" or that suggest a "substantial risk that the harm will occur."

Return to Table of Contents

## New York Court Tackles Contractual Risk of Loss Issues in Data Breach Case

**In *Jetro Holdings LLC v. MasterCard*, the New York State Supreme Court rejected a wholesaler's attempt to recover from MasterCard fees passed along by the wholesaler's credit card processor in connection with a data breach, reasoning the wholesaler had no contract with MasterCard and had agreed to indemnify the credit card processor. The court emphasized that contracts that place the risk of loss on the party best positioned to safeguard its own computer system are not unreasonable or inequitable.**

On May 3, 2016, a New York state court dismissed a wholesaler's breach of contract claim against MasterCard, holding that the wholesaler could not recover fees it paid to its credit card processor as a result of data breaches at the wholesaler's stores because the wholesaler was not a party to the credit card processor's agreement with MasterCard.[2] The court also held that the wholesaler's agreement to indemnify its credit card processor prohibited the wholesaler from recovering its losses from MasterCard. The decision illustrates the importance of considering potential losses arising from data breaches and cyberattacks when addressing risk of loss and indemnification provisions in contracts.

### Background and Claim

Jetro Holdings, LLC is a wholesaler of food products, household goods, and supplies for grocery retailers and restaurants. Jetro accepted MasterCard-branded cards at its stores but did not have a contract with MasterCard. Instead, Jetro's credit card processor, PNC Bank, processed payments made with MasterCard cards at Jetro stores pursuant to a contract between PNC and Jetro (the PNC Agreement). In exchange for PNC agreeing to process the payments made with MasterCard cards at Jetro stores, Jetro agreed to comply with MasterCard's standards for card members. Jetro also agreed to indemnify PNC against any future assessments or fees MasterCard might impose on PNC related to MasterCard transactions at Jetro's stores, even "in cases where MasterCard violated the [MasterCard] Standards or otherwise violated the law by imposing such assessments."

In 2011 and 2012, Jetro suffered two separate data breaches resulting from cyberattacks by third-party criminals. In both instances, MasterCard charged PNC nearly $7 million in fees and penalties for PNC's alleged violations of the MasterCard standards. Pursuant to the indemnity clause in the PNC Agreement, PNC withheld that amount from Jetro.

In June, 2015, Jetro filed suit against MasterCard to recover the amounts withheld by PNC. Jetro asserted claims for breach of the contract between PNC and MasterCard, breach of good faith and unjust enrichment. Jetro alleged that MasterCard violated its contract with PNC by imposing fines and that MasterCard should reimburse Jetro for the entire sum PNC withheld from Jetro.

### The Court's Decision

The New York State Supreme Court dismissed Jetro's claims. The court held that Jetro did not have standing to sue MasterCard directly on behalf of PNC because Jetro did not have a contractual agreement with MasterCard. The court also held that

[2] *Jetro Holdings LLC v. MasterCard International Inc. et al.*, case number 60374/2015, in the Supreme Court of the State of New York, County of Westchester.

the PNC Agreement prohibited Jetro from seeking reimbursement from MasterCard for Jetro's indemnification of PNC. The court ruled that "Jetro's inability to seek redress for the withholding of funds by PNC is attributable to Jetro's own agreement, in its contract with PNC, that Jetro would indemnify PNC even for assessments that might violate the data security standards or which are otherwise unlawful." In so ruling, the court reasoned: "That Jetro bargained away its remedy against PNC does not give it the right to proceed directly against MasterCard." The court rejected Jetro's argument that MasterCard was primarily liable for the fees imposed on PNC, holding that cyberhackers were primarily responsible, and that "[s]ince Jetro was in the best position to safeguard its computer system, contractual agreements which place the risk of loss on Jetro are not unreasonable, unfair, or inequitable."

### Key Takeaway

This decision highlights the importance of considering the potential financial impact of data breaches and cybersecurity during contract negotiations. Courts like the New York State Supreme Court are unlikely to rewrite liability provisions in contracts, preferring to enforce negotiated agreements as written. Companies should carefully negotiate contractual arrangements regarding indemnification with an eye toward any potential cybersecurity issues, even those that could result from third-party criminals. When entering into contracts, companies should ensure that they have considered which party will be liable in the event of a data breach.

Return to Table of Contents

## EU Data Protection Supervisor Adds to Criticism of the Privacy Shield

**The European data protection supervisor has issued an opinion that is critical of the Privacy Shield.**

On May 30, 2016, European Data Protection Supervisor Giovanni Buttarelli issued an opinion citing serious concerns about the Privacy Shield, adding to the growing chorus of critics of the data transfer regime that the European Union and United States proposed in February 2016 to replace the Safe Harbor agreement. Buttarelli's role as an independent supervisory authority is to protect personal data and privacy and promote good privacy practices in EU institutions.

While the opinion issued by Buttarelli's office praises some aspects of the Privacy Shield, such as the willingness of U.S. authorities to be more transparent regarding their use of personal data in surveillance practices, it states that the Privacy Shield is not sufficiently robust to protect the rights of EU data subjects. As we reported in April 2016, the Article 29 Working Party, a European data protection advisory body whose membership comprises representatives from the data protection authority of each EU member state, released a report critiquing certain aspects of the Privacy Shield.[3] Buttarelli's report echoes many of the same concerns set forth in the Article 29 Working Party report and offers recommendations for improving the Privacy Shield. It emphasizes the need for the Privacy Shield to be forward-looking so that companies that transfer data from the EU do not need to change compliance models repeatedly, and it points out that the Privacy Shield is based on Directive 95/46/EC, the current EU data protection directive, which will be superseded by the General Data Protection Regulation in May 2018.

### Background

EU data protection law forbids the transfer of personal information from an EU member state to a jurisdiction that does not — in the EU's view — provide "adequate" protections for that information. The EU has long viewed the United States as a jurisdiction that does not meet EU standards for data protection. In addition to certain other mechanisms to allow personal data to flow from the EU to the U.S., the two sides agreed on the Safe Harbor program, under which companies that self-certified to certain data protection standards could transfer personal information into the United States.

In October 2015, however, the Court of Justice of the European Union invalidated the Safe Harbor in *Schrems v. Data Protection Commissioner*[4] on the grounds that it did not adequately protect the interests of data subjects. The court's primary objections were the ability of the U.S. government to access personal data for national security purposes and the lack of recourse available to EU residents who felt their privacy rights had been violated fundamentally.[5] The *Schrems* decision threw into doubt the data practices of many companies, and EU and U.S. officials entered into negotiations to craft a replacement for the Safe Harbor. That replacement, the Privacy Shield, was released in February 2016.

The Privacy Shield consists of a series of key privacy principles with which companies must comply that are generally similar to those embodied in the Safe Harbor. In addition, U.S. government entities will undertake certain commitments regarding the use of

[3] See our April 2016 *Privacy & Cybersecurity Update* for more on the Article 29 Working Party report.

[4] Case number C-362/14, in the Court of Justice of the European Union.

[5] For more on the *Schrems* decision, see our special October 7, 2015, edition of *Privacy & Cybersecurity Update*.

data for national security purposes. The framework also provides new avenues of recourse for European residents who believe their data has been misused and adds more rigorous enforcement mechanisms.[6]

Before being formally adopted by the European Union, the Privacy Shield must be approved by a qualified majority of the Article 31 Committee, which is composed of EU member state representatives, after which the EU College of Commissioners must formally adopt the decision. This process is expected to be completed in June 2016.

### Recommendations

Buttarelli's opinion offers several main recommendations for improvement of the Privacy Shield:

- The Privacy Shield must be revised, as it does not offer substantially equivalent protection to Directive 95/46/EC in the areas of data retention and automated processing as currently proposed. The opinion also states that the Privacy Shield is not sufficiently clear regarding the purpose limitation or the exceptions to its requirements.
- The Privacy Shield should clarify the circumstances in which exceptions may be made for purposes of national security, law enforcement or the public interest, or in cases where the Privacy Shield conflicts with other applicable law.
- The role of the ombudsperson should be independent from both the intelligence community and any other authority, and the ombudsperson should report directly to U.S. Congress. The opinion also recommends that the EU be involved in assessing the oversight system for the processing by U.S. authorities of personal data collected from EU data subjects.

### Next Steps

It is unclear what effect the Buttarelli opinion, together with the Article 29 Working Party report, may have on the decision-making of the Article 31 Committee. The committee still can issue a binding "adequacy decision" supporting the Privacy Shield, and the EU College of Commissioners may adopt the decision, each without doing anything to address the concerns of Buttarelli or the Article 29 Working Party. However, it may be difficult for the Article 31 Committee to determine that the Privacy Shield is adequate in the face of growing criticism from EU data protection experts.

Return to Table of Contents

[6] For more on the Privacy Shield, see our February 2016 *Privacy & Cybersecurity Update*.

## Irish Data Protection Commissioner Asks European Court to Review Model Contracts

**The Irish data protection commissioner will ask the Court of Justice of the European Union to determine whether model contracts are a valid mechanism to transfer personal data from the EU to the U.S.**

When the Court of Justice of the European Union (CJEU), the EU's highest court, invalidated the U.S.-EU Safe Harbor in the *Schrems* decision in October 2015, many observed that the court's logic might also suggest that the model contracts, on which thousands of companies rely to transfer personal data from the EU to the U.S., might also not be valid. Companies and privacy advocates will now see whether that logic applies. The office of the Irish data protection commissioner (IDPC) announced on May 25, 2016, that it would ask the CJEU to determine the validity of the model contracts used by Facebook (which is the same model contract used by thousands of other companies). If the CJEU were to decide that model contracts may no longer be used as a transfer mechanism, companies could be left with few practical alternatives for transfer of such data, which could significantly disrupt business activities until a new transfer mechanism is approved.

Facebook, like a number of other multinational companies, has its EU corporate headquarters in Dublin and so is regulated by the IDPC. The IDPC has been investigating Facebook's privacy practices since Max Schrems, an Austrian privacy activist, filed a complaint alleging that the Safe Harbor transfer mechanism did not adequately protect the privacy rights of EU citizens. That complaint resulted in the CJEU invalidating the Safe Harbor. The proposed replacement transfer mechanism for the Safe Harbor, the Privacy Shield, has been met with criticism by various data protection experts, including the Article 29 Working Party and the European data protection supervisor. (See "EU Data Protection Supervisor Adds to Criticism of the Privacy Shield" on page 4 for further background on the *Schrems* case and the Privacy Shield.)

### Next Steps

The Article 31 Committee is expected to complete its review of the Privacy Shield in June 2016. If approved, the EU College of Commissioners is expected to adopt the Privacy Shield soon after. If that process is delayed, however, and the CJEU invalidates the model contract transfer mechanism prior to adoption of the Privacy Shield, companies that rely on model contracts to transfer personal data from the EU will quickly need to identify and implement an alternative transfer mechanism in order to

avoid business interruptions. Moreover, even if the Privacy Shield is adopted, many more companies have relied on model contracts than on the Safe Harbor, which the Privacy Shield would replace. A decision that the model contracts are not valid could create business havoc. Some have reasoned that the model contracts are more likely to withstand the court's scrutiny since they were drafted by the European Commission as opposed to the Safe Harbor, which was a negotiated agreement between the EU and the U.S. Whether this is false optimism remains to be seen.

Return to Table of Contents

## Insurer Pursues Subrogation Action Against Third Parties for Alleged Failure to Prevent Insured's Data Breach

**In a recent subrogation action, a Delaware court allowed the insurer to proceed with some of its claims against the defendants arising out of an alleged failure to identify and prevent a data breach sustained by its insured, signaling that some insurers are covering cyber-related losses but seeking to pass off the cost of data breaches to third parties through subrogation.**

### Background

A recent decision by the Delaware Superior Court adds to the body of case law concerning insurance coverage for cyber-related losses and suggests that at least some insurers are paying out cyber-related claims rather than contesting coverage and turning to subrogation to recoup their losses in certain situations. In *National Union Fire Insurance Co. of Pittsburgh, Pa. v. Trustwave Holdings, Inc., et al.*,[7] the court permitted National Union to proceed with some of its claims and seek discovery pertaining to certain dismissed claims in a subrogation action it filed against Trustwave Holdings, Inc., et al. alleging that Trustwave failed to prevent a data breach by National Union's insured, Euronet Worldwide, Inc.

Euronet is a global credit card payment and transaction processing company that transmits point-of-sale credit card data to credit card companies. Euronet protects the transmitted credit card data on a highly secured network designed to comply with Payment Card Industry Data Security Standard (PCI DSS) requirements and security assessment procedures promulgated by major credit card companies. PCI DSS requires Euronet to have a qualified security assessor confirm its compliance with PCI DSS on an annual basis. To this end, Euronet retained Trustwave as its qualified security assessor, entering into contracts in 2006 and 2011 pursuant to which Trustwave performed yearly PCI DSS compliance assessments, vulnerability scans and network penetration services. As part of these audits, Trustwave was required, among other things, to ensure that credit card data was encrypted and to verify that antivirus software was operable. After every audit, it confirmed that Euronet was in full compliance with PCI DSS requirements.

In December 2011, however, Euronet discovered that it had been hacked at some point during the term of the Trustwave contracts. A software vendor had failed to turn on an encryption tool, leaving stored credit card data unencrypted. Then malware was introduced to Euronet's secured network and swiped the unencrypted credit card data. The security breach affected approximately 2 million credit card numbers. Euronet paid out approximately $6 million in damages, which National Union covered under the terms of the insurance policy it issued to Euronet.

### National Union's Claims

In October 2014, National Union, as subrogee of Euronet, commenced suit against Trustwave alleging that the breach would not have occurred if Trustwave had not mistakenly told Euronet that its network was secure. On Trustwave's motion to dismiss, the court dismissed National Union's implied warranty of accuracy claims against Trustwave, finding that they failed as a matter of law because Delaware did not recognize such a claim and, even if it did, both contracts expressly disclaimed all implied warranties. Although it also dismissed the claims alleged against one of the defendants, Trustwave Holdings, Inc., on the basis that National Union failed to distinguish its alleged conduct from the other Trustwave entities, it did so without prejudice and permitted National Union to seek discovery as to which Trustwave entities undertook what responsibilities with respect to the contracts with Euronet.

Trustwave also sought dismissal of four claims against it based on improper venue, arguing that the claims in question arose out of the 2011 contract, which contained a forum-selection clause requiring that all actions relating to the contract be brought in the Courts of England and Wales. National Union countered that Delaware was the proper venue based on a Delaware forum-selection clause in the 2006 contract and that the claims in question did not arise in 2011 because the alleged 2011 conduct was part of a pattern of misconduct that began in 2006 when the parties initially contracted. The court declined to dismiss the four claims at issue, finding that dismissal was premature in light of the fact that it was unclear as to when the alleged breach or breaches occurred. However, the court indicated that it may revisit the issue in the future, stating that "[f]ollowing discovery, if it appears that the alleged 2011 conduct was separate and distinct, and not in a continuous course from 2006 onward, the Court will

[7] No. N14C-10-160 MMJ (CCLD), 2016 WL 2354621 (Del. Super. May 3, 2016).

consider whether to sever the 2011 claims to allow Trustwave to litigate in the Court of England and Wales."

### Key Takeaway

It remains to be seen whether subrogation will become commonplace in the context of cyber-related losses. Nevertheless, given the fact that insurers are litigating disputes arising out of cyber-related losses with increasing frequency, the trend appears to be that insurers are seeking to pass off the cost of cyber incidents to third parties where possible. Against this backdrop, companies of all types, including those that provide cyber/privacy services to others, should review their insurance programs to ensure that adequate coverage is in place for cyber-related liability.

Return to Table of Contents

## FTC and FCC Launch Parallel Inquiries Into Mobile Device Security Updates

**The FTC and the FCC have launched coordinated inquiries into the security practices of mobile carriers and device manufacturers.**

On May 9, 2016, the Federal Trade Commission (FTC) and the Federal Communications Commission's (FCC) Wireless Telecommunications Bureau launched parallel inquiries into the practices of various mobile carriers and mobile device manufacturers relating to mobile device security updates. The agencies' coordination is unusual and may signal future collaboration with respect to privacy and cybersecurity regulation in this area.

Historically, the FTC and FCC have not worked together on privacy and technological security issues, although they announced an intent to do so in a November 2015 joint memorandum of understanding.[8] The unique nature of the "mobile ecosystem" may require the joint efforts of both agencies. The mobile ecosystem includes phone makers, carrier companies and third-party suppliers of operating systems, and the FTC and FCC have differing regulatory authority with respect to those entities. The FTC has a broad mandate to protect consumer welfare. The FCC's regulatory scope, in contrast, focuses on regulation of communications channels, including regulation of common carriers, which the FTC does not have the authority to regulate.

In its public announcement of the coordinated inquiries, the FCC focused on Stagefright, a bug discovered in July 2016 that facilitated attacks on Android phones via text message. Google began issuing monthly security updates for Android after Stagefright was discovered, but a significant number of Android users failed to receive timely deliveries of those updates — in part due to carrier delays in supplying those updates. The FCC stated that the failure to promptly and consistently deliver security patches across all mobile devices leaves consumers unprotected.

The recipients of the inquiries reflect each agency's scope of authority. The FTC sent its requests to eight mobile device manufacturers,[9] and its questions address in detail the state of smartphone and tablet vulnerabilities and the processes for patching them. The manufacturers must provide information that includes:

- the factors that they consider in deciding whether to patch a vulnerability on a particular mobile device;
- detailed data on the specific mobile devices they have offered for sale to consumers since August 2013;
- the vulnerabilities that have affected those devices; and
- whether and when the company patched such vulnerabilities.

Meanwhile, the FCC directed its inquiry to six communications carriers[10] and focused on how the carriers review and release security updates. Its 20 questions cover obstacles to releasing updates, whether carriers know if customers install updates and Stagefright-specific vulnerabilities. Collectively, the companies contacted by the two agencies were chosen because they manufacture or provide operating systems for the majority of devices in the United States.

### Key Takeaway

The FTC and FCC have not indicated what they intend to do with the information they gather, but the specific nature of the questions suggests that they may issue more targeted guidance with respect to mobile device security. In any event, the announcement of the parallel inquiries suggests that they may work together in the future to regulate mobile devices.

Return to Table of Contents

[8] See our November 2015 *Privacy & Cybersecurity Update* for a summary of the memorandum of understanding.

[9] The eight companies that received orders from the FTC are: Apple, Inc., Blackberry Corp., Google, Inc., HTC America, Inc., LG Electronics USA, Inc., Microsoft Corp., Motorola Mobility, LLC and Samsung Electronics America, Inc. See the May 9, 2016, FTC press release "FTC to Study Mobile Device Industry's Security Update Practices" for more on the inquiries.

[10] The six companies that received inquiries from the FCC are: AT&T, Verizon Communications Inc., T-Mobile USA Inc., Sprint Corp., U.S. Cellular and Tracfone Wireless Inc.

## Banking Associations Publish 'International Cybersecurity, Data and Technology Principles'

**The European Banking Federation, Global Financial Markets Association, and International Swaps and Derivatives Association collaborated on and have issued a set of cybersecurity principles that are designed to guide global policy-making in the financial industry.**

On May 9, 2016, the European Banking Federation (EBF), Global Financial Markets Association (GFMA, which is comprised of the Asia Securities Industry & Financial Markets Association, Association for Financial Markets in Europe and Securities Industry and Financial Markets Association) and International Swaps and Derivatives Association (ISDA) released a set of common principles on cybersecurity, data and technology that they intend as a guide for countries, regulatory agencies and standards-setting bodies to use in developing global standards and policy in the financial services industry. Underlying the principles are two core themes: first, that the risks associated with cybersecurity, data and technology transcend borders and thus require global solutions; and second, that effective regulations and standards must take into account the rapidly shifting nature of technology and associated cybersecurity threats.

### Global Threats Require Global Solutions

The principles begin by acknowledging that, although global financial systems are heavily intertwined, firms operating in the financial sector are subject to diverse and sometimes conflicting laws and regulations. In response, the principles advocate development of standards, guidelines and regulations at an international level, cautioning against localized rules that may "inadvertently force global businesses to fragment their technology systems, impeding competition and innovation and thereby harming investors." Instead, policymakers and stakeholders should seek to establish global approaches that encourage "open, safe and interoperable" financial technology ecosystems through an open and transparent process. The principles identify PCI DSS as a key example of the potential for internationally accepted standards to minimize risk through widespread implementation, while noting that encryption standards and source code disclosure requirements present topics on which a more cohesive international standard could be crucial.

The principles stress in particular the limiting effect that onerous restrictions on data flows can have on global financial systems and security. While the obligation to protect customer data is globally recognized within the industry, policymakers must also consider that data sharing and monitoring of customer activity can be essential to detecting cybercrime, and that transmitting and storing data across national boundaries is "fundamental to supporting a global financial system that is capable of enabling the goals of national economies and the industries that comprise them." Thus, the principles call for a balance between privacy and security.

### Evolving Technology Requires Flexible Standards

In addition to the global nature of cybersecurity, data and technology issues, the principles highlight the rapidly evolving nature of both the threats and solutions posed by technology. Accordingly, although the principles call for international solutions, they also caution against a "one-size-fits-all approach to cybersecurity." Rather than designing policies based on specific, rigid technology requirements, which the principles argue are primarily reactive and quickly outdated, regulations should "enable programs that are risk-based, threat-informed, and based on the size, scope, function and business model of the entity being regulated." Effective regulations should "ensure that sufficient people, processes and technology are in place to manage risks" while leaving companies room to determine the exact technology to best meet their particular security needs, risk appetite and business objectives. The principles also emphasize the importance of seeking practical input from stakeholders so that the resulting regulations are effective and do not result in unintended consequences.

### Starting a Conversation

Through these principles, the participating entities hope to facilitate conversation and cooperation among government and private sector institutions, with the ultimate goal of developing "safeguards that protect the integrity of global markets." To spearhead this conversation, the EBF, GFMA and ISDA are seeking the input of two international standard-setting organizations, the Financial Stability Board and the International Organization of Securities Commissions.

Return to Table of Contents

## New York Attorney General Reports Significant Increase in Data Breach Notices, Implements Online Submission Form

**The number of data breach notices the New York attorney general's office has received in the first five months of 2016 is an increase of more than 40 percent over the same period last year. The office has implemented an online submission form to streamline the notice process for companies.**

New York Attorney General Eric T. Schneiderman announced that his office had received 459 data breach notices involving New Yorkers for the year as of May 2, 2016, which is an increase of more than 40 percent over the 327 notices received by the same time last year. His office received 809 data breach notices total in 2015 and expects to receive well over 1,000 notices this year, which would be a new record.

Any company that experiences a data breach that concerns the private information of a New York state resident must alert the attorney general's office and the affected consumer pursuant to New York's Information Security Breach and Notification Act. In order to streamline the notice process, the attorney general's office now provides companies with the ability to file data breach notices via an online submission form.

Return to Table of Contents

## EU Antitrust Authorities Discuss Relevance of Privacy in Competition Law

**The French and German competition agencies have published a joint report on big data and its implications for competition law.**

On May 10, 2016, the French Competition Authority and German Federal Cartel Office published "Competition Law and Data," a joint report on big data and its implications for competition law. The paper identifies issues that antitrust authorities should consider when assessing the interplay among big data, market power and competition law. While privacy was not a main focus of the paper, the antitrust authorities discussed ways in which privacy considerations may be relevant for purposes of antitrust analysis.

### Relevance of Big Data for Antitrust Analysis

The term "big data" refers to increasingly large data sets collected by companies on the basis of their activities via the web, social networking or intelligent devices. Due to the volume of those data sets, the processing of big data requires specific tools and processes. The emergence of big data is the result of the exponential growth both in the availability and automated use of information, which has prompted the development of complex analytics based on algorithms to spot patterns. Companies collect and analyze this data to improve the quality and level of their services as well as to offer more targeted advertising services.

The report has identified a number of potentially anti-competitive practices that can arise in the context of the acquisition, accumulation and use of big data. According to the report, privacy practices are not, in and of themselves, within the scope of regulation by competition authorities, nor have privacy practices been used to date as a significant indicator of competition in the competition authorities' practice. However, privacy protection may raise competition law concerns in certain cases, as discussed below.

### Mergers and Acquisitions

The report discusses potential antitrust issues raised by big data in the context of acquisitions of companies that own large sets of consumer data. The report identifies both horizontal issues — the concentration of data that results from a merger of two firms active in the collection and sale of big data — and nonhorizontal issues, described as potential foreclosure effects arising from mergers between companies active in vertically or otherwise related activities of the big data value chain (*e.g.*, data collection and online targeted advertising). The European Commission looked at these potential effects, for example, in the Facebook/WhatsApp deal, and in particular whether the transaction would increase the concentration of data within Facebook's control to the extent that it would enable Facebook to strengthen its position in the area of online targeted advertising. In that case, the commission determined there was no cause for such concern because WhatsApp does not collect or store data on its users.

The report also stated that privacy issues would be especially relevant to a merger control analysis if a company benefits from strong market power toward its end users. If two companies obtain strong market power through a merger, the combined entity could further increase its market power through increased collection of data from its end users, reducing the privacy of such end users. The report notes that some analysts have equated a reduction in privacy to a reduction in product quality, which could be considered for merger control purposes.

### Conduct

In the area of conduct, the report identifies as the key issue whether the collection of big data can give companies the ability to foreclose or marginalize other competitors active in the

markets where big data is used through practices such as refusing to provide access to data that is essential for the conduct of a competitor's business, entering into exclusive arrangements with third-party data providers and conditioning access to data on the use of the data holder's own data analytics services.

In addition to such practices, the report discussed the ways in which privacy practices may impact such an analysis. For example, the report noted that competition law concerns arise whenever a dominant company, for which data is a main input for its products or services, clearly breaches data protection laws. This is the concern the German Federal Cartel Office raised when, on March 2, 2016, it announced the opening of an investigation against Facebook for an alleged abuse of its dominant position by infringing data protection rules.[11] The report stated that privacy practices could also be used by the competition authorities as a means of assessing exploitative conduct, particularly in cases where terms and conditions are imposed on consumers and consumers are unlikely to read such terms and conditions.

### Key Takeaway

Competition agencies around Europe are paying ever-increasing attention to big data and have begun the process of trying to understand the role of data in corporate strategies and the possible application of competition law to such strategies. While the competition authorities to date have not focused on privacy practices as part of their analysis, the report signals that they may begin to do so in the near future.

[11] See our March 11, 2016, client alert "German Competition Regulator Investigates Facebook for Alleged Violation of Data Protection Laws."

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

**James R. 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

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

**Timothy G. Reynolds**
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

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

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

**Michael Y. Scudder**
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

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

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

**Gregoire Bertrou**
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

**Joshua F. Gruenspecht**
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com