Skadden

Privacy & Cybersecurity Update

FTC Administrative Law Judge Holds FTC Must Show More Than 'Possibility' of Harm

A Federal Trade Commission administrative law judge has held that the FTC must show more than the mere "possibility" of harm arising from a cybersecurity incident in order to sustain a Section 5 case; a decision with potentially far-reaching impact on the cases the FTC will bring.

In a decision that could have broad implications for the type of cybersecurity cases brought by the Federal Trade Commission (FTC), an FTC administrative law judge has held that a "possibility" of future harm to consumers arising from a cybersecurity incident is insufficient to sustain a Section 5 claim by the FTC. The November 13, 2015, decision by FTC Chief Administrative Law Judge Michael Chappell dismissed the FTC's complaint against LabMD,[1] marking the end — for now — of a protracted battle between the agency and an Atlanta-based cancer detection company that shut down during the course of the case.

Background

The LabMD case arose from a somewhat unusual "cyberbreach" fact pattern. The complaint by the FTC alleged two separate security incidents affecting LabMD, but neither involved consumers actually being subject to identity theft or other harm. The first incident took place in 2008, when a 1,718 page file containing personal data related to approximately 9,300 LabMD patients was inadvertently uploaded to LimeWire, a peer-to-peer file sharing site (the 1718 File). The 1718 File was found on LimeWire by Tiversa, an infosecurity company that, at least in part, locates potential activities of this type and then sells its cybersecurity services to affected companies. When LabMD refused to purchase Tiversa's services, Tiversa turned its findings over to the FTC.

The second incident was uncovered in 2012 when law enforcement officers in Sacramento, California, found documents containing information for approximately 600 LabMD customers in the possession of identity thieves (the Sacramento Documents).

[1] *In the matter of LabMD, Inc.,* Docket No. 9357 (FTC, November 13, 2015).

There was no evidence any of the individuals whose information was in the 1718 File or the Sacramento Documents actually were subject to identity theft or other harm, nor was there any evidence that the Sacramento Documents were derived from the 1718 File.

The FTC's complaint alleged that LabMD failed to take adequate cybersecurity measures, and that the consumers whose information appeared in the 1718 File or the Sacramento Documents were subject to an increased risk of identity theft harm, as well as "significant risk" of reputational harm, privacy harm or other harms caused by the unauthorized exposure of medical information. In addition, the FTC argued that all consumers whose information was maintained on LabMD's computer network were subject to an increased risk of identity theft as a result of LabMD's failure to maintain adequate safeguards against data breaches.

In analyzing the FTC's claim, Judge Chappell focused on the meaning of "likely" harm to consumers, which is required to sustain a claim under Section 5 of the FTC Act. According to Judge Chappell, "likely" means that harm to consumers must be probable, not merely possible, and that the FTC must show "more than hypothetical or theoretical harm." Here, the judge found that the FTC's allegations were all premised on possible harm that might befall LabMD customers. For example, there was no evidence that the 1718 File had even been accessed by a third party, and significant time had elapsed since the file had been posted without any evidence of identity theft or other harm to consumers. In response to the FTC's claims that identity theft could take months or years to actually manifest, Chappell held that "[f]airness dictates that reality must trump speculation based on mere opinion." In this respect, Judge Chappell's opinion tracks the reasoning of a Nevada district court in a putative class action brought against Zappos. In that case as well, the judge was hard-pressed to find any harm to consumers giving the long period of time since the incident had occurred, without any reports of identity theft or other harm.[2]

Chappell also found that the "risk" of harm from unreasonable data security practices, without more, was insufficient to establish a Section 5 violation. As Chappell noted, under the FTC's interpretation "everyone is 'at risk' at every moment, with respect to every danger which may possibly occur."

[2] For example, in June, a Nevada judge dismissed claims against Zappos for lack of an adequate showing of harm to consumers. The circumstances were similar to the LabMD case, where a period of time had passed without any actual identity theft or other harm to consumers. *In re Zappos.com, Inc., Customer Data Security Breach Litigation*, 3:12-cv-00325-RCJ-VPC, Dkt. 235 (D. Nev. June 1, 2015).

Practical Implications

In a number of cybersecurity cases brought by the FTC, there is little dispute that consumers face actual or probable harm. In these case, there is proof of access to personal information by hackers or reports of fraudulent charges or misuse of information. In this respect, the LabMD case presented an unusual fact pattern. First, the FTC was informed about LabMD's cybersecurity practices through Tiversa, which was acting in effect as a "whistleblower." Second, LabMD personal information was indeed sitting out in the open, but the company was fortunate that no one had actually accessed the file. Nonetheless, Judge Chappell's decision was sweeping in its analysis of "likelihood" of injury. The FTC may therefore hesitate from bringing cases against companies where there is only a possibility of harm to consumers. The decision also provides those companies who believe there was no harm to their consumers with a basis to challenge an FTC action.

The timing of the decision is also significant in that it comes on the heels of the FTC's victory in its case against Wyndham hotels.[3] In that case, the Third Circuit held that the FTC had the authority to challenge a company's cybersecurity practices under the "unfairness" prong of Section 5, even if the company had not engaged in any deceptive practices.[4] Many saw *Wyndham* as providing the FTC with broad authority to pursue companies for their cybersecurity practices. While Judge Chappell's decision does not affect the specific ruling of Wyndham, it does mean that in such "unfair" practice cases, the FTC will need to show probable (and not just "possible") harm to the consumer.

The LabMD case might also have two indirect impacts as well. First, Judge Chappell was particularly critical of the FTC's reliance on Tiversa — a company that searches peer-to-peer sites for company files and then attempts to "monetize" such files by selling its services. Chappell's focus on the veracity of Tiversa's testimony (such as claims the 1718 File was accessed, when in fact it was not) and concerns about incentivizing this business model may cause the FTC to shy away from partnering with such companies in finding cybersecurity threats.

Second, the decision could impact the current negotiations between the U.S. and EU regarding the transfer of data from Europe to the U.S.[5] Historically, when the EU has critiqued the U.S. for lacking any meaningful privacy enforcement body, the U.S. has pointed to the FTC's authority in this space. Any

[3] *Federal Trade Commission v. Wyndham Worldwide Corp. et al.* (3d Cir), No. 14-3514.

[4] See our November 2014 *Privacy & Cybersecurity Update* for a more complete description of that decision.

[5] See our October 2015 *Privacy & Cybersecurity Update*.

decision that limits the FTC's authority at this critical juncture in the negotiations could have an intangible adverse impact.

As of the date of this mailing, the FTC is deciding whether to appeal the decision to the commissioners of the FTC.

Return to Table of Contents

European Commission Releases Guidance on Transatlantic Data Transfers After *Schrems* Rejection of US-EU Safe Harbor

The European Commission has issued guidance on how companies should respond to last month's EU decision invalidating the U.S.- EU Safe Harbor.

On November 6, 2105, one month after the Court of Justice of the European Union invalidated the U.S.-EU Safe Harbor in its *Schrems* ruling, the European Commission issued guidance concerning transatlantic data transfers in the wake of the monumental decision. After providing background on the now-invalid Safe Harbor and the effect of the *Schrems* ruling, the commission's "explanatory communication" outlines alternative mechanisms currently available for the transfer of personal data to the United States and offers a glimpse into negotiations of a new Safe Harbor.

Alternative Transfer Mechanisms

Unless and until a new Safe Harbor is recognized, companies must rely on alternative mechanisms in order to transfer data to the United States in compliance with the *Schrems* ruling.

The commission's guidance largely echoes and confirms the statement issued on October 16, 2015, by the Article 29 Working Party, the independent advisory body including representatives of all data protection authorities of Member States and the European Data Protection Supervisor, and confirms the continuing validity of standard contractual clauses, binding corporate resolutions and express derogations as mechanisms of transatlantic data transfer.

Standard Contractual Clauses. The commission has approved four sets of standard contract clauses specifying data protection obligations — two for transfers between data controllers and two for transfers between a controller and processor — that may be incorporated to compensate where a country has not been found to have an adequate general level of data protection. Data subjects may enforce the rights they derive from these contractual clauses as third-party beneficiaries before national data protection authorities and courts of the Member State in which a data exporter is established.

Because commission decisions are binding in their entirety, national data protection authorities in principle may not refuse the transfer of data to a third country on the sole basis that they do not find the standard contractual clauses to offer sufficient protection. However, these authorities may review the clauses and their implementation in particular instances and may seek a preliminary ruling against their use from the Court of Justice. Some data protection authorities additionally maintain a system of notification or pre-authorization for use of standard contractual clauses. Because using standard contractual clauses places companies under the supervision of data protection authorities, companies are advised to be familiar with the authorities and any guidance they have issued in the Member States in which they operate. Companies also may seek data protection authority approval of ad hoc contractual arrangements on a case-by-case basis.

Binding Corporate Resolutions. Companies may adopt a single set of binding and enforceable rules within a corporate group in order to facilitate transfer of data among affiliates without the need to have contractual arrangements between each entity. The rules must accord with the substantive and procedural requirements laid out by the Article 29 Working Party, and, similar to standard contractual clauses, are enforceable in the EU by individual data subjects in their capacity as third-party beneficiaries.

Transfers on the basis of binding corporate resolutions must be authorized by the data protection authority in each Member State from which the corporation intends to transfer data, and corporations must designate an entity in the EU to accept liability for breaches of the rules. The Article 29 Working Party has established a standardized application form and procedure to ease this process, but many companies nonetheless find it to be a cumbersome process.

Derogations. Irrespective of the use of standard contractual clauses or binding corporate rules, personal data may be transferred to third countries to the extent that the transfer falls under several narrowly construed exceptions in Article 26(1) of Directive 95/46/EC. Express derogations include such transfers as those that are necessary for the performance of a contract with or in the interest of the data subject and those for which the data subject has given unambiguous consent.

A New Safe Harbor?

While these alternative mechanisms will have to suffice for the short term, the commission considers it crucial to establish a simple, effective and comprehensive framework with commitments and enforcement by the U.S. authorities. In its view, only a comprehensive framework can ensure the level of data protection afforded Europeans under EU data protection law for the volume of data transfers in the modern commercial world. The commission accordingly hopes to conclude negotiations with the

U.S. government by the end of January 2016, coinciding with the end of the "grace period" granted by the Article 29 Working Party before data protection regulators will begin to take enforcement actions.

Prior to the *Schrems* ruling, the commission already had begun to review and discuss the Safe Harbor with U.S. authorities. These negotiations, started in 2013, have continued with renewed vigor following the ruling. Negotiations are focused around 13 commission recommendations that pertain to increased transparency of privacy practices, improved data subject access to alternative dispute resolution, more robust enforcement of the Safe Harbor and limited access to personal data by U.S. authorities. The commission indicates that there is "agreement in principle" to the transparency, redress and enforcement recommendations, but that details must still be worked out in order to ensure that any new framework will be binding enough to meet the requirements that the court laid out in *Schrems*.

The commission envisions that the new system will include more active involvement by national data protection authorities, who will play a role in the review of the functioning of the system through an improved and more direct relationship with the U.S. Department of Commerce. It also is working to establish an annual joint review of any new framework with the United States in order to ensure that any adequacy decision will remain valid.

While the commission claims to have committed to the January time frame to conclude the current negotiations, it notably does not indicate that there has been any agreement, even "in principle," with regards to the final set of recommendations on data access by U.S. authorities. As inadequacies in this particular area largely formed the basis of the *Schrems* decision, failure to agree upon a framework with sufficient limitations, safeguards and judicial control mechanisms in place against possible access by U.S. authorities for law enforcement and national security purposes may prevent the neat solution that the commission seeks. With this possibility in mind, companies should continue to use alternative mechanisms and keep abreast of guidance and developments regarding the adequacy of those mechanisms and any amendments that may be necessary.

Other Adequacy Decisions

The commission has, over time, found that a few countries provide adequate data protection such that transfers form the EU to that country are permissible without the need for additional steps (like the model contracts). Argentina, Canada, Israel, New Zealand and Switzerland are the most noteworthy of these countries. The *Schrems* court, while not questioning the commission's ultimate "adequacy" decision for these countries, noted that in each case, the commission improperly limited the power of the (Data Protection Act) DPA to overrule its adequacy finding. According to the court, DPAs must always remain empowered to examine, with complete independence, whether data transfers to a third country comply with the requirements laid down by the EU Data Directive. In its recent guidance, the commission indicated that it would remove any such limitation it had imposed on the DPAs.

The commission's communication may be found here, the press release here and its Q&A summary here.

Return to Table of Contents

NYDFS Opens Conversation on Financial Services Cybersecurity Framework

Moving into the next stage in its campaign to take on a larger role in regulating the cybersecurity of financial institutions, the New York State Department of Financial Services has released a letter laying out its initial thoughts regarding cybersecurity regulations for the financial services sector and has invited other federal and state regulators to join the agency in developing a comprehensive approach.

On November 9, 2015, the New York State Department of Financial Services (NYDFS) released a letter it had sent to a number of federal and state financial regulators discussing its plan to consider comprehensive cybersecurity regulations for financial institutions. After years of investigating cybersecurity practices at financial institutions subject to NYDFS authority, the agency states that it is now considering requiring those institutions to comply with a series of regulatory requirements ranging from maintaining cybersecurity policies to notifying the NYDFS of incidents. The NYDFS indicated that its letter was intended to "spark additional dialogue" and expressed its desire to work with other regulators to "develop a comprehensive cybersecurity framework that addresses the most critical issues," while preserving its right to address additional state-specific concerns.

After summarizing its recent reviews of cybersecurity practices, the NYDFS listed some key conclusions. Among them were that while "financial institutions have taken significant steps to bolster cyber security efforts in recent years, companies will continue to be challenged" by malicious actors and that "the scale and breadth of the most recent breaches and incidents demonstrate that cyber security is a global concern that affects every industry at all levels." As a result, the agency feels that the time is ripe to step in with financial services regulation in order to fill a "demonstrated need" in the industry.

The letter then described a series of concrete requirements that the NYDFS is considering as part of a mandatory cybersecurity program "designed to perform core cyber security functions" for "covered" financial institutions, including:

- **Maintaining Policies and Procedures.** Implementing and maintaining written policies and procedures addressing core cybersecurity areas ranging from information security to incident response.
- **Third-Party IT Vendor Oversight.** Developing policies, procedures and standard contractual language to address third-party vendor-related concerns such as keeping data stored offsite encrypted and providing proper incident notification.
- **Multi-factor Authentication.** Requiring multi-factor authentication across a range of access points to financial institution networks, from customer-facing to vendor-facing.
- **Chief Information Security Officer (CISO).** Designating a CISO whose responsibilities would include, among others, submitting an annual report to NYDFS.
- **Application Security.** Implementing and periodically refreshing application security standards.
- **Internal Expertise.** Employing personnel adequate to the task of managing cyber risk.
- **Auditing.** Conducting annual penetration testing and quarterly vulnerability assessments and maintaining a logging trail for auditability.
- **Notice of Incidents.** Providing notice to NYDFS of any cyber incident with "a reasonable likelihood of materially affecting" normal operations.

The NYDFS described its proposals as "the product of the Department's analysis and discussion … to date," but indicated that additional proposals may be forthcoming. While the agency continues its work, it is simultaneously inviting feedback from other regulators in the hopes of spurring all parties' interest in "develop[ing] a comprehensive approach to cyber security regulation in the weeks and months ahead."

Return to Table of Contents

FCC Will Not Require Websites to Honor 'Do Not Track' Requests

The Federal Communications Commission has dismissed a petition by Consumer Watchdog that would have required "edge providers" such as Google and Facebook to comply with a user's request not to be tracked.

On November 6, 2015, the Federal Communications Commission (FCC) dismissed a consumer advocacy group's petition asking the FCC to apply Section 222 of the Communications Act to "edge providers." Edge providers are individuals or companies that provide content, applications or services over the Internet. Large edge providers are companies like Google, Facebook, YouTube, Netflix, but nearly any company or individual on the Internet could be an edge provider. Section 222 of the Communications Act protects private information gained by telephone companies by virtue of providing telephone services, and the Open Internet Order extends that protection to private information collected by ISPs. The advocacy group, Consumer Watchdog, wanted the FCC to extend the Open Internet Order to edge providers and require them to comply with a user's request not to be tracked. The so-called "do not track" technology would allow a user to click a button in the user's browser settings to prevent a website from tracking the user's browsing activities. Accordingly, the expansion of the Open Internet Order to edge providers would have drastically expanded the entities subject to Section 222.

Ultimately, the FCC declared that it has been "unequivocal" in declaring that such edge providers are not regulated by the FCC. The FCC pointed to its earlier statement in the Open Internet Order that it was not "regulating the Internet, *per se*, or any Internet applications or content" to support its statement that it does not intend to regulate edge providers. The FCC dismissed the petition without seeking further comment.

Return to Table of Contents

Consumer Electronics Association Releases Best Practices For Privacy and Security of Personal Wellness Data

In late October 2015, the Consumer Electronics Association released guiding principles governing the collection, storage and use of personal wellness data, including that which is collected by the growing number of wearable devices that have become popular with consumers over the past several years.

Wellness-related wearable devices that track users' calories, steps, heart rate and other health information represent a rapidly growing industry, and with it, a rapidly growing base of consumer data and analytics. In light of this trend, the Consumer Electronics Association (CEA) released "Guiding Principles on the Privacy and Security of Personal Wellness Data" on

October 20, 2015.[6] These voluntary best practices provide baseline recommendations to obtain and maintain consumer trust and are applicable to a broad range of companies that offer services or products that collect, store or use personal wellness data. The guidance is arranged under the eight themes summarized below.

- **Security.** Because consumers tend to have higher expectations of security surrounding personal wellness data, CEA recommends that companies ensure that their security measures are "reasonable and proportional to the sensitivity of that data." Companies may employ administrative, physical and technical safeguards and should arrange for vendors and suppliers handling the data to have similarly robust security.
- **Policy and Practice.** Consumers will be more comfortable using health-related devices when they understand how their information is stored and used. The guidelines state that companies should maintain a written policy explaining how they collect, store, use and transfer personal wellness data, addressing foreseeable security risks and ensuring compliance with applicable laws.
- **Concise Notice.** Maintaining a privacy policy alone will not necessarily enable consumers to understand how their personal wellness data is collected and used. The guidelines state that companies should endeavor to provide clear and concise summaries of their policies. The CEA recommends exploring creative and accessible formats, potentially using graphics, icons, charts, video or audio.
- **Unaffiliated Third Party Transfers.** Because consumers seek transparency about and control over transfer of their personal wellness data, the guidelines state that companies should seek affirmative consent if they intend to transfer personal wellness data to unaffiliated third parties. The CEA notes that one initial consent should suffice for subsequent transfers to the same entity, unless the requested type or proposed use of personal wellness data materially changes. Users should have the ability to revoke consent at any time.
- **Fairness.** Recognizing the rising proliferation of data analytics, the CEA recommends that companies be wary of the possibility that these analytics could create unjust or prejudicial outcomes for consumers. In order to guard against this risk, companies may periodically review algorithms and other automated decision methodologies, in addition to refraining from knowingly using personal wellness data in unjust or prejudicial ways. This is particularly important where the data will be used to determine eligibility for critical benefits or services, such as employment, health care, financial products or services, credit, housing or insurance.
- **Personal Data Review, Correction and Deletion.** Continuing on the theme of user control, companies should make available means to review and correct their personal wellness data. This is also particularly important where a company intends to share the information with a third party that will determine the user's eligibility for critical benefits or services referenced above. The CEA further encourages companies to allow users to request deletion or de-identification of personal wellness data. Companies should comply with, and require vendors, suppliers and other service providers to comply with such requests where feasible.
- **Advertising Communications.** The CEA recommends that companies who tailor advertising provide a way for users to opt out of use of their personal wellness data for this purpose and obtain affirmative user consent before transferring data to a third party who will use the data for their own advertising purposes.
- **Law Enforcement Response.** The guidelines state that privacy policies should describe when and how the company will respond to lawful requests for a user's personal wellness data from civil and law enforcement agencies.

Conclusion

While some of the themes of the CEA's guidelines are familiar, such as the recommendations that companies have adequate security measures and privacy policies in place, other themes are less common and may reflect evolving consumer expectations around data privacy and security. For example, the guideline that calls for obtaining affirmative consumer consent prior to transferring personal wellness data to an unaffiliated third party goes beyond the more universal requirement simply to provide notice to consumers of such transfer, and may strike some companies as overly burdensome. Similarly, it will be interesting to see whether the guideline requiring a summary of the privacy policy in addition to the privacy policy itself will be adopted more widely. While compliance with the guidelines is voluntary, companies that collect, store and process personal wellness data should familiarize themselves with the guidelines and consider carefully any business practices that deviate from them.

Return to Table of Contents

FTC and FCC Sign Memorandum of Understanding For Continued Cooperation on Consumer Protection Issues

The FTC and FCC recently came to an agreement on how to cooperate on consumer protection issues, which will have an important impact on data security enforcement.

On November 16, 2015, the FTC and FCC signed a Memorandum of Understanding (MoU) to cooperate on consumer protection issues. While written in broad terms, many see it as a way

[6] The guidelines are available in full here.

to end a simmering dispute as to which agency would pursue privacy and cybersecurity matters. Over the last 18 months, the FTC brought its first enforcement action against a mobile carrier, alleging it had engaged in fraudulent "cramming" billing, while the FCC issued a fine against a cellphone company for failing to protect its consumers' personal information.

The MoU does not give one agency primacy over the other with respect to cybersecurity matters, nor does it require an agency to step aside if the other has taken the lead. Rather, the MoU is directed towards cooperation so that the actions of one agency do not hamper the other, with the goal of avoiding "duplicative, redundant, or inconsistent oversight in areas [of consumer protection], building upon their long history of cooperation on matters of overlapping authority." The key provisions of the MoU include the following:

- coordination of agency initiatives where one agency's action will have a significant effect on the other agency's authority or programs;
- consultation on investigations or actions that implicate the jurisdiction of the other agency;
- regular coordination meetings;
- sharing of relevant investigative techniques and best practices; and
- engaging in joint enforcement actions, when appropriate and consistent with their respective jurisdictions.

The MoU also states that the FTC can pursue common carriers in their non-common carrier activities.

Return to Table of Contents

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

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@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