4 QUESTIONS YOU NEED TO ASK ABOUT FTC ENFORCEMENT ACTIONS ON DATA PRIVACY VIOLATIONS

BY MARCIE ERNST

IN THE UNITED STATES, *the Federal Trade Commission (FTC) serves as the primary federal enforcer of consumer data privacy and security laws for most businesses. Companies that violate privacy rights of consumers or mishandle sensitive consumer information may face legal enforcement actions brought by the FTC and state-level authorities. The FTC began to bring these actions in the late 1990s and has since established a wealth of its own privacy jurisprudence in the absence of many judicial decisions relating to FTC enforcement. Together with various state-level agencies, the FTC has successfully investigated and taken legal action against many companies that have been alleged to have mishandled personal consumer information. Here are four key considerations you need to be aware of in ensuring compliance.*

1. What is the scope of FTC authority to enforce consumer privacy and security?

Within the FTC's Bureau of Consumer Protection, the Division of Privacy and Identity Protection is responsible for consumer privacy enforcement. In the early stages of its involvement in data privacy enforcement, the FTC simply enforced regulations created by companies for themselves, pursuant to its authority under Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[1] The FTC's authority has expanded over the years to include enforcement of key portions of the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework, and the Children's Online Privacy Protection Act of 1998 (COPPA).

2. How does the FTC's self-regulatory regime work?

Under the FTC's self-regulatory regime, companies are required to disclose their privacy policies to consumers and abide by their stated policies. Two pillars of the self-regulatory system emerged from the Fair Information Practice Principles issued in the 1970s by the U.S. Department of Health, Education, and Welfare: notice and choice.

Companies generally provide notice to their consumers of how their information is collected, stored and transferred through a privacy policy. A consumer must then consent to those terms. This is often accomplished through a right to opt out, but is more strongly supported by an affirmative opt-in by the consumer.

3. Are FTC enforcement actions effective?

As a consumer data protection authority, the FTC has been criticized as being weak and lacking teeth, particularly compared to data protection authorities in other countries. Many other nations have established government agencies with designated authority to enforce data privacy laws, whereas the development of the FTC into a data protection authority was much less deliberate. Undoubtedly, data privacy and security laws in the European Union are stronger and more developed than the body of applicable law in the United States.

In fact, disapproval by EU leaders of the inadequacy of data privacy laws and enforcement in the United States was the impetus of the U.S.-EU Safe Harbor Framework, implemented in 2000. The Safe Harbor Framework provided a legal mechanism for companies to transfer consumer data between the EU and U.S., after EU leaders passed legislation prohibiting ▶

CASE STUDIES

RECENT FTC ENFORCEMENT ACTIONS

HIGH-PROFILE CASES OF PRIVACY VIOLATION

Uber Technologies

The scenario: In August 2018, the FTC announced an expanded settlement with Uber Technologies for its alleged failure to reasonably secure sensitive data in the cloud, resulting in a data breach of 600,000 names and driver's license numbers, 22 million names and phone numbers, and more than 25 million names and email addresses.

The settlement: The expanded settlement is a result of Uber's failure to disclose a significant data breach that occurred in 2016 while the FTC was conducting its investigation that led to the original settlement. The revised proposed order includes provisions requiring Uber to disclose any future consumer data breaches, submit all reports for third-party audits of Uber's privacy policy and retain reports on unauthorized access to consumer data.[2]

Emp Media Inc. (Myex.com)

The scenario: The FTC joined forces with the State of Nevada to address privacy issues arising from the "revenge" pornography website, Myex.com, run by Emp Media Inc. The website allowed individuals to submit intimate photos of the victims, including personal information such as name, address, phone number and social media accounts. If a victim wanted their photos and information removed from the website, the defendants reportedly charged fees of $499 to $2,800 to do so.

The settlement: On June 15, 2018, the enforcement action brought by the FTC led to a shutdown of the website and permanently prohibited the defendants from posting intimate photos and personal information of other individuals without their consent. The defendants were also ordered to pay more than $2 million.[3]

Lenovo and Vizio

The scenario: In 2018, FTC enforcement actions led to large settlements with technology manufacturers Lenovo and Vizio. The Lenovo settlement related to allegations the company sold computers in the U.S. with pre-installed software that sent consumer information to third parties without the knowledge of the users. With the New Jersey Office of Attorney General, the FTC also brought an enforcement action against Vizio, a manufacturer of "smart" televisions. Vizio entered into a settlement to resolve allegations it installed software on its televisions to collect consumer data without the knowledge or consent of consumers and sold the data to third parties.

The settlement: Lenovo entered into a consent agreement to resolve the allegations through a decision and order issued by the FTC. The company was ordered to obtain affirmative consent from consumers before running the software on their computers and implement a software security program on preloaded software for the next 20 years.[4] Vizio agreed to pay $2.2 million, delete the collected data, disclose all data collection and sharing practices, obtain express consent from consumers to collect or share their data, and implement a data security program.[5]

VTech

The scenario: The FTC's action against toy manufacturer VTech was the first time the FTC became involved in a children's privacy and security matter.

The settlement: In January 2018, the company entered into a settlement to pay $650,000 to resolve allegations it collected personal information from children without obtaining parental consent, in violation of COPPA. VTech was also required to implement a data security program that is subject to audits for the next 20 years.[6]

LabMD

The scenario: LabMD, a cancer-screening company, was accused by the FTC of failing to reasonably protect consumers' medical information and other personal data. Identity thieves allegedly obtained sensitive data on LabMD consumers due to the company's failure to properly safeguard it. The billing information of 9,000 consumers was also compromised.

The settlement: After years of litigation, the case was heard before the U.S. Court of Appeals for the Eleventh Circuit. LabMD argued, in part, that data security falls outside of the FTC's mandate over unfair practices. The Eleventh Circuit issued a decision in June 2018 that, while not stripping the FTC of authority to police data security, did challenge the remedy imposed by the FTC.[7] The court ruled that the cease-and-desist order issued by the FTC against LabMD was unenforceable because the order required the company to implement a data security program that needed to adhere to a standard of "reasonableness" that was too vague.[8]

The ruling points to the need for the FTC to provide greater specificity in its cease-and-desist orders about what is required by companies that allegedly fail to safeguard consumer data.

Despite criticism of its regulatory inadequacy, the FTC has brought legal action against many businesses, addressing many data privacy issues.

member nations from transferring data to countries with inadequate privacy protection. Following a finding by the European Court of Justice in 2015 that the Safe Harbor Framework did not provide an adequate level of privacy protections, the U.S. and EU renegotiated and improved upon the Framework, replacing it with the EU-U.S. Privacy Shield Framework in 2016.

Despite criticism of its regulatory inadequacy, the FTC has successfully brought legal actions against many businesses addressing a wide range of data privacy issues including peer-to-peer file sharing, social media networking, spam, spyware, behavioral advertising and failure to adhere to privacy commitments.

4. What is the future of FTC enforcement actions?

The FTC's approach to enforcement actions against companies that fail to properly handle consumer data will likely shift to imposing more customized conditions. Under the Eleventh Circuit's decision in *LabMD*, specific benchmarks for data security, rather than vague standards of "reasonableness," will be required for companies accused of failing to safeguard data. Given the speed of innovation, defining "reasonableness" for each individual company may prove challenging for the FTC.

As the U.S. looks forward in its approach to consumer data privacy protection, there may be a trend toward aligning U.S. data privacy laws and enforcement measures with the robust body of law in this area in the EU. If that trend develops, it is likely that the FTC will need to be empowered with even more regulatory powers with a clearer congressional mandate.

Marcie Ernst is a partner in SGR's Litigation Practice. She has extensive experience in commercial litigation at trial and appellate court levels. Her practice also includes cybersecurity, data privacy and technology matters. **mernst@sgrlaw.com**.

Endnotes

1. 15 U.S.C. § 45(a)(1).
2. www.ftc.gov/news-events/press-releases/2018/04/uber-agrees-expanded-settlement-ftc-related-privacy-security.
3. www.ftc.gov/system/files/documents/cases/emp_order_granting_default_judgment_6-22-18.pdf.
4. www.ftc.gov/news-events/press-releases/2018/01/ftc-gives-final-approval-lenovo-settlement.
5. www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.
6. www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.
7. The United States Court of Appeals for the Third Circuit has rejected this argument. *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 247-49 (2015).
8. www.media.ca11.uscourts.gov/opinions/pub/files/201616270.pdf.