Federal Trade Commission Issues Privacy and Data Security Report for 2017

By Nicole Ewart and Reed Freeman

On January 18th, the Federal Trade Commission ("FTC") released its Annual Privacy and Data Security Update, recapping its enforcement actions, workshops, and other privacy and data security activities in 2017.

Enforcement highlights from 2017 include the FTC's settlement with Vizio, Inc. and a large joint enforcement effort with 32 State Attorneys General against Lenovo. Vizio agreed to pay a $2.2 million civil penalty to settle the FTC's allegations that it had installed software on its TVs to collect consumers' viewing data without consumers' knowledge or consent and then sold such data to third parties for targeted advertising (among other purposes). This complaint and settlement marked the first time that the FTC took the position that television viewing information is "sensitive information," for which companies must obtain opt-in consent from consumers. In Lenovo, the FTC and the states alleged that Lenovo sold laptops with preinstalled software that accessed consumers' sensitive personal information transmitted over the internet without consumers' knowledge or consent. Lenovo's settlement of the enforcement action, which requires it to implement and maintain a comprehensive software security program subject to biennial third-party audits for 20 years, was approved by the FTC on January 2, 2018.. Also in 2017, the FTC (through the Department of Justice) achieved a significant civil penalty award against Dish Network for alleged violations of the FTC's Telemarketing Sales Rule, including alleged Do Not Call and abandoned call violations.

Notably, international data transfer pacts were an enforcement focus area for the FTC in 2017. The FTC took action against three companies that allegedly misrepresented their EU-US Privacy Shield Certification status, all allegedly claiming they were certified under the data transfer framework, when in actuality, according to the FTC's allegations, all three failed to complete the Privacy Shield certification process. Along similar lines, three other companies settled actions for allegedly misrepresenting their participation in the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APEC CPBR) System. Other companies that faced FTC enforcement actions last year include: Uber, Upromise, and TaxSlayer, among others.

On the data security front, the Acting Chairman signaled a revisiting of the use of the Commission's unfairness authority, under Section 5(n) of the FTC Act, calling for a showing of concrete consumer injury in the cases the FTC decides to litigate. Ms. Ohlhausen has stressed that a "focus on consumer harm is part of [the FTC's] statutory mandate, but is also good policy." She noted that the FTC's data security cases "are on the strongest legal and policy footing when they address clear and concrete consumer injury." The Commission followed-up on this with a workshop on informational injury in December, where it examined consumer injury in the context of privacy and data security; discussions included how to characterize and measure such injuries.

In its data security litigation with D-Link Systems the FTC alleged in a complaint initially filed in January 2017, and filed unredacted in March 2017, that inadequate security measures left wireless routers and internet cameras vulnerable to attack. (Notably, the Commission vote authorizing the staff to file the complaint. was 2-1, with Commissioner [not yet Acting]

Ohlhausen voting no.) The FTC's complaint asserted both unfairness and deception claims against D-Link, alleging that despite promoting the security of its routers, D-Link failed to take steps to address well-known and easily preventable security flaws. Notably, the FTC did not claim that any customer data was exposed or that any breach had occurred. In the ensuing litigation, D-Link contended that no "substantial injury" occurred or was likely to occur, as required for an unfairness claim under Section 5(n) of the FTC Act, in the absence of evidence of actual exposure or misuse of any data. In September 2017, the district court dismissed the FTC's unfairness claim (as well as two of the five deception allegations) against D-Link in light of the FTC's failure to allege any concrete facts of actual harm to consumers. The matter, which is ongoing, will be one to watch in 2018.

Beyond enforcement, while 2017 was a relatively quiet year on the rulemaking and review front for the FTC (the FTC reviewed its Gramm Leach Bliley Act Safeguards Rule, initiated a review of the CAN-SPAM Rule, and reviewed and reissued, unchanged, its Fair Credit Reporting Act Disposal Rule), the FTC was actively involved in industry events and business and consumer education. The Commission hosted a number of events and workshops covering topics from identity theft, to artificial intelligence and block chain, to peer-to-peer payment systems and crowdfunding, and connected cars. (Our blog post on the FTC's take-aways on that workshop is here.)

The FTC also maintained active consumer and business blogs in 2017. For example, the Commission launched its very detailed Stick with Security blog series, expanding on and providing insight into the FTC's Start with Security business guidance issued in 2015.

The FTC also provided and updated guidance for businesses on a range of topics, such as:

- how the NIST Cybersecurity Framework aligns with the FTC's work on data security;
- how to respond to a phishing scam;
- how businesses can defend against ransomware;
- steps companies should take to respond to a data breach; and
- how businesses can comply with COPPA.

Finally, in 2017 the FTC continued to engage and cooperate with foreign data protection authorities around the world. The Commission, along with the Department of Commerce and others, participated in the first annual review of the EU-US Privacy Shield Framework, and the FTC designated a liaison to assist EU data protection authorities with inquires on Privacy Shield participants' compliance with the framework and its principles. Beyond the EU, the Commission hosted delegations and engaged in bilateral discussions with officials from the Canada, China, Japan, Korea, Singapore and the UK on data privacy and security issues.

In 2018, expect to see continued FTC engagement with businesses, consumers, and foreign authorities. Look for enforcement actions involving the Privacy Shield, so that the FTC can demonstrate that it is serious about the pact, in preparation for the next annual review. Also look for more garden-variety deception cases involving misrepresentations or material omissions in statements about privacy or data security, and data security cases alleging unfairness only when the Commission can prove concrete harm. To that end, it will be interesting to see what comes from the FTC's informational injury workshop.