FTC Issues 2018 Year in Review

MARCH 18, 2019

On Friday, March 15, 2019, the Federal Trade Commission released its *Privacy & Data Security Update: 2018*, highlighting its privacy and data security enforcement actions and other activities last year.

Notable Privacy Enforcement Actions

On the privacy side, one of the FTC's largest actions involved a joint effort with the state of Nevada to obtain a final court order against MyEx.com, an alleged revenge porn website. The order shut down the website and required the operators to pay $2 million in equitable monetary relief. Other enforcement actions in 2018 included an action against PayPal related to the privacy settings and the data security of its payment servicer Venmo. Notably, at least two of the FTC's privacy actions involved coordination with state agencies. In addition to MyEx.com noted above, which was a joint action with the Attorney General of Nevada, the FTC coordinated with the New York Attorney General's Office in an action against Hylan Asset Management, LLC regarding an alleged scheme to collect fake and unauthorized debts from consumers.

Notable Data Security Enforcement Actions

The FTC's notable enforcement actions include a complaint and settlement against BLU Products, Inc., a mobile phone manufacturer. The FTC alleged that despite company claims that it maintained "appropriate" data security, BLU failed to implement appropriate procedures to oversee its service providers' security practices. The FTC claimed that preinstalled software on the BLU devices provided by its service providers contained common security vulnerabilities that could enable malicious actors to gain full access to the devices. The FTC also settled charges with toymaker VTech Electronics Limited over the company's alleged failure to use reasonable and appropriate data security, including by failing to implement adequate safeguards with respect to its collection of personal information through the Kid Connect mobile application. The FTC further alleged that the company failed to encrypt personal information submitted by users despite statements that it did. VTech's settlement requires the company to implement a comprehensive data security program and obtain independent audits every other year for 20 years. Notably, the VTech action was a joint effort, this time an international joint effort: the FTC collaborated with the Office of the Privacy Commissioner of Canada, which issued its own Report of Findings against VTech for the

company's inadequate security measures.

The VTech settlement also include remedies for alleged COPPA violations. The FTC alleged that VTech collected personal information from children without providing direct notice and obtaining parental consent. VTech agreed to pay $650,000 as part of its settlement for those alleged violations. Similarly, on the COPPA front, the FTC obtained a $235,000 civil penalty against Explore Talent for alleged COPPA violations, and issued warning letters to notifying smart watch makers based in China and Sweden that their watches marketed to U.S. children must comply with COPPA.

As has become standard practice, 2018 saw the FTC bring a handful of enforcement actions against companies claiming EU-U.S. Privacy Shield certification or compliance. The FTC brought actions against five companies that allegedly either failed to complete the certification process or allowed their certifications to lapse despite statements that they complied with the Framework. The FTC also participated in the second annual review of the Framework.

On the telemarketing front, the FTC brought a number of actions for alleged violations of the Telemarketing Sales Rule related to unauthorized robocalls and calls to consumers on the Do Not Call Registry. Notably, the FTC filed a lawsuit (*FTC v. James Christiano*, No. SA CV 18-0936, C.D. Cal.) against two related operations that allegedly facilitated billions of illegal robocalls, including to hundreds of millions of numbers on the federal Do Not Call Registry. One of the defendants has settled to date.

FTC Advocacy

The report further highlights the FTC's advocacy work during 2018, including its testimony before the House and Senate on privacy and data security issues, federal privacy legislation, and enforcement of the Fair Credit Reporting Act. The FTC also submitted comments to the Consumer Product Safety Commission related to internet-connected consumer products and to the National Telecommunications and Information Administration (NTIA) on privacy as part of NTIA's consumer privacy proceeding.

2018 Rulemaking Activity

On the rulemaking front, in 2018 the FTC announced a regulatory review of the Red Flags Rule, which requires financial institutions to maintain identity theft protection programs. In seeking public comments on whether the FTC should update the Rule, the FTC noted that identity theft was the second biggest category of consumer complaints in 2017, and the third biggest source of complaints through the first three quarters of 2018. And, in November 2018, the FTC issued a Notice of Proposed Rulemaking related to Congress's May amendment to the Fair Credit Reporting Act requiring nationwide consumer reporting agencies to provide free credit monitoring for active duty military.

Workshops, Publications, and Education Initiatives

Finally, the Report highlights the FTC's 2018 workshops, publications, and consumer and business education efforts, including the FTC's third annual PrivacyCon held in February. Issues covered

during the workshops included Internet of Things, AI, cryptocurrency, big data, privacy and competition, and data security. With respect to reports and guidance, the FTC released a report on Mobile Security Updates, related to mobile security and mobile system patching, and also issued the Staff's perspective on a December 2017 workshop on informational injuries consumers may suffer from privacy and security incidents. In addition, the FTC continues to maintain and update its consumer and business blogs.

Significantly in 2018, the FTC initiated its Hearings on Competition and Consumer Protection in the 21st Century, which will continue through 2019. These hearings are likely to result in a report that will inform the FTC's enforcement and related activities for privacy, data security, and competition going forward. A report could be issued by the end of this year.

Notable hearings for privacy and data security in 2018 included:

- September 13, 2018: Review of Competition and Consumer Protection Landscape; Concentration and Competitiveness in U.S. Economy; Privacy Regulation
- September 21, 2018: State of U.S. Antitrust Law; Mergers and Monopsony or Buyer Power
- November 6-8, 2018: Privacy, Big Data, and Competition
- November 13-14, 2018: Algorithms, Artificial Intelligence, and Predictive Analytics
- December 11-12, 2018: Data security

Upcoming hearings include:

- March 20, 2019: Competition and Consumer Protection Issues in U.S. Broadband Markets
- March 25-26, 2019: The FTC's Role in a Changing World
- March 25, 2019: Roundtable with the State Attorneys General
- April 9-10, 2019: The FTC's Approach to Consumer Privacy

Notable 2019 Activities to Date

Turning to 2019, the FTC has already secured the largest COPPA settlement in its history against Musical.ly, obtaining a $5.7 million civil penalty for the company's failure to provide appropriate direct notice to parents and obtain parental consent, among other things. The FTC has also concluded its regulatory review of the CAN-SPAM Rule, which it began in 2017, leaving the Rule unchanged, and has proposed changes to the Safeguards Rule and Privacy Rule under the Gramm-Leach-Bliley Act.

Going forward, we can expect to see the FTC actively engaged in discussions around federal privacy legislation as the topic receives more focus from Congress. Data security will continue to loom large in 2019 as major data breaches continue to fill news headlines and as the Internet of Things and connected devices explode in size. Joint efforts among the FTC and states or international agencies will also likely expand as states play a more active role in enforcing consumer privacy and data security laws. All signs point to an interesting and busy year on the privacy and data security front.

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP