Cybersecurity Law Report
An Acuris company

How Facebook's $5-Billion FTC Settlement Is Shaping Compliance Expectations

By Rebecca Hughes Parker, *Cybersecurity Law Report*

Facebook's FTC settlement includes the largest fine ever levied for data privacy violations, and an unprecedented remedial order that mandates a board-level privacy committee and heightened privacy requirements, among other things. We look at how this monumental resolution, which had strong dissents from two FTC Commissioners, is shaping the data privacy enforcement climate, the specific obligations in the order and compliance takeaways. In a future article, we will examine the social media giant's $100-million SEC settlement based on allegations that it was misleading in its public disclosures about improper use of data. See "Learning From the Equifax Settlement" (Jul. 31, 2019).

Enforcement Appetite and the Demand for Legislation

The $5-billion FTC Facebook settlement, coming on the heels of the $575-million FTC Equifax settlement and the announcement by the U.K. Information Commissioner's Office (ICO) of large proposed fines on British Airways and Marriott following breaches, has changed the enforcement landscape for data privacy and data security. These actions "signal a new era of aggressive data privacy and data security enforcement on both sides of the Atlantic," Joseph Facciponti, a partner at Murphy & McGonigle, told the Cybersecurity Law Report.

The Equifax and Facebook cases together "are landmark cases that usher in a new era for the FTC in flexing its muscle in privacy and data security matters," Lisa Sotto, a partner at Hunton, argued. There is an increasing awareness in the government and in the public in general of "the enormous power of big data and the concomitant potential for

misuse and harm such that this is just the tip of the iceberg," Una Dean, a partner at Fried Frank, told the Cybersecurity Law Report. "We will see more enforcement actions down the line, whether from the FTC or other agencies," she added.

The FTC Order (Order) is centered around Facebook's violation of a previous FTC Order (the 2012 Order). It charges violations of Section 5 of the FTC Act. Among other things, it requires Facebook to adopt policies and procedures going forward regarding representations of data use, sharing of nonpublic user information, the deletion of certain information, use of telephone numbers given for multi-factor authentication purposes, enhanced security around passwords and new facial recognition templates. It also mandates a privacy program and requires independent privacy program assessments, including a board-level committee and the reporting of certain incidents to the FTC.

The propriety of the Order is hotly debated – Commissioner Rohit Chopra and Commissioner Rebecca Kelly Slaughter each wrote strong dissents arguing that the Order did not go far enough in terms of the fine or the remedial measures and was just a slap on the wrist to a recidivist company with outsized global influence and revenue. They also noted that there was no individual liability. "Facebook's officers and directors were legally bound to ensure compliance with the 2012 order, yet the proposed settlement grants a gift of immunity for their failure to do so," Chopra wrote.

Facciponti said that the criticism of the settlement, including from two FTC commissioners, "reveals that there is appetite for even larger fines and even stricter requirements." The next arena, however, may be Congress. "The two lengthy dissents were certainly notable here," Dean agreed. "My sense is that those dissents will do more to spur a call for Congress to act rather than impact future enforcement actions and settlements by the FTC," she told the Cybersecurity Law Report.

Dean also noted that she frequently hears privacy professionals "lament that the lack of clear guidance in the U.S. around acceptable data privacy practices is a source of great confusion when setting up privacy programs." Thus, she believes more people "will begin to demand legislative action in this space to create greater predictability and uniformity."

See "Implications of Nevada's New Privacy Law" (Jul. 10, 2019).

Never Waste a Crisis

The latest cases and heightened awareness around data privacy present a good opportunity to sell boards on the importance of strong

privacy programs. "Clearly, the FTC and SEC, as well as the public, have made plain that their patience with opaque and misleading data privacy and usage practices has worn thin," Dean said. "Privacy is the order of the day, and it is gaining increased attention at the C-suite and board levels."

Recent settlements have grabbed the attention of boards in an unprecedented way, Sotto said. "I have probably spoken to about 40 boards about cybersecurity issues and for the first time about a month ago, a board asked me to address data privacy. I was surprised by that, but the dollar amounts that have been bandied about – not just in the U.S. but also in the U.K. with the proposed penalties for British Airways and Marriott – are enough to demand the attention of boards and C-suites everywhere."

See "Privacy Officers Share Best Practices for Reporting to the Board" (Jul. 24, 2019).

Unusual or Justified Immunity?

Notably, Dean said, the Order "resolves all claims, whether known or unknown, related to Facebook's alleged violation of the 2012 consent order," and though settlement agreements do cover conduct not specifically related to the allegations at hand, "those provisions typically follow an investigation and identification of the specific conduct for which immunity is being provided. I'm not sure I've ever seen a settlement that provides immunity for unidentified misconduct." The remedial steps in the order, including the stringent privacy program now mandated, may have convinced the FTC that even unknown prior conduct will be addressed, she reasoned.

The FTC dissenters were not convinced, however. "A release of this scope is unjustified by our investigation and unsupported by either precedent or sound public policy," Slaughter argued in her dissent. Chopra wrote: "I have not been able to find a single Commission order – certainly not one against a repeat offender – that contains a release as broad as this one."

The day after the FTC settlement was announced, the Electronic Privacy Information Center (EPIC) filed a motion to intervene in the case to block judicial approval of the Order. Among its arguments is that the settlement releases Facebook from liability for past violations, extinguishes more than 26,000 consumer complaints and does not limit the amount of data that Facebook can harvest.

See our three-part series on lessons from the FTC's 2018 Privacy and Data Security Update: "Enforcement Takeaways" (Apr. 24, 2019); "Financial Privacy, COPPA and International Enforcement"

(May 1, 2019); and "Hearings, Reports and 2019 Predictions" (May 8, 2019).

New Settlement Model

Regardless of whether it goes far enough, the Order does set a new framework for FTC settlements and "provides a model for what the FTC would consider to be a strong privacy program for businesses that engage in the processing of large amounts of personal data," Facciponti said.

The details in both the Facebook and Equifax orders are a change from the "formulaic settlements of the past. They are highly tailored and extremely prescriptive in addressing the particular issues that they seek to remediate," Sotto said, adding that the settlement formula previously used by the FTC "is probably a thing of the past and the FTC has signaled that it is going to be looking for more bespoke settlements – so that the settlements going forward will be more pinpointed in addressing the specific claims that the government is alleging."

The Stipulated Order

The Order was filed in District Court for the District of Columbia on July 24, 2019, along with a Complaint that states it "seeks to hold Facebook accountable for its failure to protect consumers' privacy as required by the 2012 Order and the FTC Act." The 2012 Order resolved various allegations, including that Facebook was giving developers access to the data of friends of app users without permission. The Complaint details the numerous violations of the 2012 Order, which are reflected in the various remedial actions the current Order demands.

The elements of the Order do not break new ground themselves. "Many of the provisions of the Order – such as the requirement for Facebook to be candid with its users in how it uses their data or to establish a comprehensive privacy policy," Facciponti observed, "merely track Facebook's obligations under the FTC Act and other laws and is consistent with the 'notice and consent' model of privacy in the U.S."

See "Equifax and Facebook Settlements Overshadow More Routine FTC Summer Settlements" (Jul. 24, 2019).

Prohibition Against Misrepresentations

The Order requires that Facebook not misrepresent, "expressly or by implication," its maintenance of the security and privacy of "Covered Information," as the Complaint charges that it did in the past. Covered Information is defined to include a broad swath of personal information including "geolocation information sufficient to identify a street name and name of city or town" and "IP address, User ID or other persistent identifier that can be used to recognize a User over time and across different devices."

Facebook cannot mislead users, for example, about "the extent to which a consumer can control the privacy of any Covered Information" and the steps to implement those controls, as well as the extent to which Facebook has made data accessible to third parties.

See "Takeaways From the U.K. ICO's FaceApp Warning" (Jul. 31, 2019).

Changes to Sharing of Nonpublic User Information

The Order prohibits Facebook from sharing the nonpublic information of a user with a third party without clear and conspicuous disclosure and affirmative express consent.

See "Utah Act Increases Restrictions on Access to Third-Party Data" (Apr. 10, 2019).

Deletion of Information

Facebook must make sure information that a user has deleted is not available to a third party within 30 days of deletion. It also must ensure that Covered Information that Facebook controls is deleted or de-identified within 120 days. There are a few exceptions to this, such as for safety, security and technical feasibility.

See "Best Practices for Managing the Risks of Big Data and Web Scraping" (Jul. 26, 2017).

Limitations on Phone Number Sharing

Facebook is also prohibited from using a phone number provided for a security purpose – such as for multi-factor authentication – to sell advertisements or otherwise sharing the number with a third party.

See "Overcoming the Challenges and Reaping the Benefits of Multi-Factor Authentication in the Financial Sector (Part One of Two)" (Jul. 26, 2017); Part Two (Aug. 9, 2017).

Mandated Privacy Program

The Order lays out provisions of a privacy program Facebook must implement within 180 days of the Order, including requirements that it:

- **Document the program.** Document the "content, implementation and maintenance of the Privacy Program" and provide that description to the Principal Executive Officer (Mark Zuckerberg) and the Independent Privacy Committee – the board-level committee, explained below – at least once a year.
- **Hire an independent privacy chief.** Designate employee(s), including a "Chief Privacy Officer for Product" (CPO), to run the program. The CPO's hiring and removal must have approval from the Independent Privacy Committee.
- **Conduct and document risk assessments.** Assess and document, at least annually, internal and external risk in each area of operations, including, within 30 days, risks relating to a Covered Incident (defined as one where Facebook has verified that the Covered Information of 500 or more users was accessed, collected, used or shared by a third party in violation of Facebook's terms).
- **Implement safeguards, including**:
    - annual third-party certifications, and monitoring and enforcement against third parties that violate contract terms;
    - privacy review of new products, services or practices, with documentation and a detailed written report about any privacy risks and safeguards, and a quarterly report from the CPO to the Principal Executive Officer (Mark Zuckerberg) of these reviews and all privacy decisions, in advance of meetings of the Independent Privacy Commission, described below;
    - controls that limit employee access to Covered Information and that protect information shared with affiliates; and
    - disclosure and consent for face recognition.
- **Test safeguards.** Safeguards must be tested, assessed and monitored annually and 30 days after a Covered Incident.
- **Implement training.** Establish regular privacy training programs.
- **Ensure the performance of service providers.** Retain providers capable of safeguarding Covered Information and contractually require them to safeguard it.
- **Use outside experts.** Seek guidance from independent third parties on implementing, maintaining and updating the program.

- **Evaluate the program.** Evaluate the program at least annually, taking into account Covered Incidents.

Sotto said these terms in full should be "carefully scrutinized by companies as they think about how they ought to enhance their own privacy programs." Though "privacy-by-design" principles have not yet been integrated into U.S. law, she observed, "this settlement is a proxy in the U.S. for the privacy-by-design standard that companies will look to in shaping their own programs."

Though there is criticism that the Order allows Facebook to retain too much power, Dean said that these provisions can still serve as a model for companies. "Any company dealing in consumer data, in particular, must engage in comprehensive risk assessments when rolling out new products and services or changing existing ones, when aggregating consumer data for revenue generation and when selling data or providing data access to third parties."

See "How GoDaddy Built an Effective Privacy Program" (Nov. 7, 2018).

Independent Privacy Program Assessments and Certifications

The Order further requires biennial assessments from third-party professionals (Assessors) who are "reasonably approved" by the Independent Privacy Committee. The Order details the contents of the assessments and requires an initial assessment 180 days after the mandated privacy program is put into place and then one every two years for 20 years.

The Assessors must sign off on the assessment and must represent that they did not "rely primary on assertions or attestations" by Facebook's management.

The Order also specifies that Zuckerberg and certain compliance officers must sign certifications annually about the privacy program.

Covered Incident Reports

Facebook must submit a report to the Assessor and to the FTC within 30 days after a Covered Incident, and follow up every 30 days until the incident is fully investigated and "any remediation efforts are fully implemented…"

This is an extension of third-party monitoring, Facciponti explained. "Most companies struggle in finding the right way to exercise effective oversight of third parties. Here, the order takes it a step further and requires Facebook to notify the FTC whenever a third party misuses Facebook data for more than 500 users."

Mandated Independent Privacy Committee

Notably, the Order contains governance requirements, including the creation of an Independent Privacy Committee comprised of Independent Directors who meet certain privacy and compliance requirements. Sotto characterized this board-level involvement as "the most important structural aspect of the settlement" and shows the FTC's intention to emphasize the tone from the top. "The settlement ensures that there will be senior-level oversight from a board committee, with the hope that the mandate from the top will trickle down," she said.

The Independent Privacy Committee is to receive a quarterly report from Facebook management about the privacy program and will meet quarterly with the Assessors. The Order also specifies how the Independent Privacy Committee will be formed and how Facebook's certificate of incorporation is to be amended.

While independent assessments are present in other FTC settlements, "the board committee is likely a response to the unique characteristics of Facebook's management structure," Facciponti said.

"If an agency perceives that a company cannot or should not be left to police itself, the goal is to shine sunlight on the company's operations through independent bodies with access," Dean explained, noting that many of the concepts in the Order are apparent in Sarbanes-Oxley and corporate monitorship agreements and are familiar in the enforcement world. "For instance, quarterly compliance certifications by a company executive; an independent privacy assessor akin to an independent financial auditor; a board committee with direct oversight responsibility; and periodic reporting of findings into the enforcement body, here the FTC: these have all been adapted from an enforcement playbook that has been around for quite a while."

Dean observed that public companies have been aggressively prioritizing cybersecurity and baking it into their business functions at the board level following the SEC's February 2018 guidance around cyber-related disclosures and governance. "Privacy should be no different. And now, companies must also be attuned to the reputational risk should unsavory data usage practices come to the public's attention. It is not simply about legal violations."

How Much Will the Order Affect Facebook?

FTC Chairman Joe Simons said the settlement is "unprecedented in the history of the FTC" and is designed "to change Facebook's entire

privacy culture to decrease the likelihood of continued violations."

Zuckerberg publicly characterized the Order as "requiring major structural changes," and outgoing general counsel Colin Stretch wrote in a blog post that compliance with the Order will require a "fundamental shift" within the company. But, Dean told us, "at the same time, and at the end of the day, there is the competing interest in delivering value to Facebook's shareholders, value that is maximized by mining and selling Facebook's key asset – data."

Facebook has been able pivot quickly in a changing landscape thus far, Dean noted. "The new privacy regime that the Order imposes will certainly have an effect on pace and potentially render Facebook less nimble. Facebook will have to find a way to continue its expansion and growth, both geographically and into new products and services while also building into its processes the elements of the Order."

See our two-part series on insights from Uber: "An Inside Look at Its Privacy Team Structure and How Legal and Tech Collaborated on Its Differential Privacy Tool" (Nov. 28, 2018); "Building Bridges Between Legal and Engineering" (Dec. 5, 2018).