Client Alert: Facebook Settles FTC Privacy Complaint for Billions: What Your Business Needs to Know

July 24, 2019

Facebook agreed today to settle FTC charges that its privacy practices violated a 2012 Consent Order. Businesses should expect increased scrutiny of their own privacy practices as a result.

The $5 billion settlement payment will be the largest the agency has ever received for consumer privacy violations. The amount will likely garner the most headlines and attention, but opinions vary as to whether a payment equal to 9% of Facebook's 2018 revenue and 23% of its 2018 profits will prove an effective deterrent.

Rather than the dollar amount, the Settlement's real legacy will likely be the privacy practices Facebook has agreed to implement. Facebook will hire outside assessors to review its privacy practices, and its executives will be accountable for the results.

After Enron, Sarbanes-Oxley changed the accountability of publicly traded companies. The new Facebook privacy regimen should raise privacy awareness in US boardrooms to a new level, and provide a standard for all companies to consider in protecting and processing personal information.

The Details

In a 2012 FTC Consent Order, Facebook agreed not to misrepresent to consumers how Facebook controlled, used or shared their personal information. In 2018, the FTC charged Facebook with violating that Consent Order.

In the 2018 Complaint, the FTC alleged, among other things, that Facebook had misled users about its sharing of personal information; had continued to allowing app developers to access users' friends data; had allowed those app developers most profitable to Facebook to violate its privacy policies; had implied to 60 million users they could opt in to facial-recognition technology when, in fact, it was already active by default; and had told users their phone numbers could enable two-factor authentication when the numbers were actually used for advertising purposes.

After a year-long investigation and extensive negotiations, Facebook agreed to a new Order, effective for 20 years. Facebook must now:

- Pay $5 billion
- Enforce its privacy policies against app developers regardless of profitability
- Expand Facebook's privacy program requirements to WhatsApp and Instagram
- Obtain opt-in consent before using or sharing personal information in new ways
- Establish a new, independent board committee focused solely on privacy
- Submit quarterly and annual certifications of privacy compliance to the FTC
- Allow monitoring by independent third-party assessors and the FTC
- Address privacy risks of new products, services or practices before implementing them
- Report any data compromises of 500 or more users within 30 days, with 30-day updates
- Hold quarterly meetings between Facebook management and the privacy committee

Two FTC commissioners dissented because they felt the $5 billion was not enough given Facebook's monetization of personal information for profit despite the 2012 Order. They also stated that the release of all FTC claims through June 12, 2019 was too generous, that Facebook's new privacy measures were not strong enough to prevent its future misuse of personal information, and the FTC should require more public disclosures from Facebook going forward under the new Order.

The Rest of the Enforcement Story

The buck does not stop with the FTC. The Securities and Exchange Commission also today announced a $100 million settlement with Facebook in the Cambridge Analytica matter, where the SEC had charged that Facebook made misleading disclosures regarding the risk of misuse of its user data.

State attorneys general can seek civil penalties on a "per violation" basis, which add up in a hurry. States are typically the first to review data breach responses and complaints from consumers about data privacy.

In addition, state consumer protection laws often permit private causes of action, including consumer class actions. For example, Cook County Illinois sued Facebook in 2018 under the Illinois Consumer Fraud Act over the Cambridge Analytica matter on behalf of affected Illinois residents. A federal court in California remanded the case to Illinois state court, where it now faces a motion to dismiss by Facebook. A private law firm is handling the class action for the County, and will receive 20% of any money Facebook pays the County.

Takeaways

In the new Order, the FTC has provided specific administrative and structural changes to corporate governance to prevent further misuse of consumer personal information. There will be a trickle-down effect. Now more than ever, all US companies should understand the rising expectations and increased liability

associated with their collection, use, and sale of consumer personal information.

- Know what personal information you have, and what your obligations are to the data subjects.
- If you receive personal information from others, keep it secure and notify the other party if there is a problem as agreed.
- Know what your vendors do to protect personal information you share with them.
- Regularly apprise your board of your risks and proactive measures regarding data.
- Adopt effective privacy and information security policies; and practice what you preach.
- Have an Incident Response Team and Plan.
- Conduct training, anti-phishing exercises, table top exercises and other measures.

For more information about data protection, contact Tedrick Housh or Jason Schwent in Lathrop Gage's Cybersecurity and Data Privacy Practice.

---

[1] *See* https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf

[2] *See* https://cookcountyrecord.com/stories/512680832-cook-county-official-argues-lawsuit-against-facebook-should-remain-in-illinois