On the WLF Legal Pulse

Timely commentary from WLF's blog

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

August 1, 2019

FTC's Facebook Settlement: What Does it Signal?

by Gerard M. Stegmaier

The Federal Trade Commission's (FTC) recent $5 billion settlement with Facebook is unprecedented in multiple respects:

- The $5 billion penalty represents the largest privacy and data security settlement in history – it is almost 20 times larger than the recent Equifax Inc. settlement and dwarfs recent EU data protection enforcement actions.
- As part of the settlement, new corporate governance measures relating to privacy and data security will be required, including an independent committee of the board of directors, with specific nomination requirements and subject matter coverage. This will place pressure on many boards and organizations to freshly examine information governance risk.
- The settlement also requires executive certifications, which, if modeled by other companies, will trigger dramatic changes in accountability as executives turn to rely on experts, internal compliance teams, audit and related expertise for assurance and attestation in order to avoid civil and criminal penalties and derivative litigation.

The signaling effect of the settlement to the broader business community intended by the primary privacy regulator in the United States cannot be overstated. Similar enforcement actions, such as individual prosecutions in Europe under the EU Data Protection Directive, triggered immediate response and attention from corporations just as the emergence of breach notification laws resulted in massive new investments in information security programs in the United States.

Summary of the settlement

The FTC accused the company of failing to adequately protect users' privacy and comply with a 2012 consent decree with the agency. Under the settlement terms, in addition to paying a $5 billion penalty and other requirements, the company must:

- Exercise greater oversight over third-party apps and app developers;
- Establish and maintain a new, comprehensive data security program;
- Complete a rigorous prerelease privacy assessment before rolling out new or modified products and services;

Gerard M. Stegmaier is a Partner in the Washington, DC office of Reed Smith LLP. This post originally appeared in the firm's *Technology Law Dispatch* and is reprinted with permission of the author.

- Subject itself to quarterly reporting and biennial assessments of its new privacy program by independent third-party assessors;
- Appoint an independent committee of the board of directors focused on privacy, which is appointed by an independent nominating committee; and
- Designate compliance officers approved by the new board committee who are tasked with ensuring and certifying privacy and data security compliance.

The company must regularly certify its compliance to the FTC, and its compliance officers and chief executive officer are subject to civil and criminal penalties resulting from false certifications.

Implications

Several aspects of the settlement are especially relevant for many businesses, especially in relation to corporate governance.

Privacy and security enforcement has (sharp) teeth. This latest settlement, along with the Equifax settlement and large fines in the EU, make clear that direct financial consequences, beyond reputational injury, will increasingly threaten organizations whose data governance practices are questioned. With dramatic new civil penalty authority becoming available in California in July of 2020 under the California Consumer Privacy Act, incentives for aggressive enforcement and related headlines could create a terrible bite for all organizations, but especially those deemed by regulators to be ill-prepared.

The Golden Rule of Privacy isn't alchemy. Many practitioners have advised clients for more than a decade that the Golden Rule of Privacy is to "do as you say and say as you do." The latest settlement highlights $5 billion reasons why now, more than ever, hostile regulators may scrutinize every statement a company makes and, where penalties are available, aggressively allege violations in the name of future deterrence. Companies whose revenue models and strategy are undeveloped or who are dependent on digital advertising and marketing will be especially at risk. The risks and consequences of data supply chain management gone awry have just increased exponentially.

Agency action reaffirms information is the asset class of the twenty-first century. In levying such a large penalty, and doing so where actual and concrete injury to consumers would have been very difficult to prove in court, the agency has set off an alert beacon warning global corporations. Those in positions of responsibility for privacy and data security can expect heightened scrutiny and accountability. At the same time, the insistence by the FTC in this case on independent board-level governance and personal executive accountability going forward represents a dramatic acceleration of changes that were set off with the EU's General Data Protection Regulation.

While there are many other subtleties to the complaint and settlement, this latest enforcement action signals something that we have said for a long time to clients. Privacy and data security risks are here to stay, and data governance and accountability risks will continue to grow in the next decade.

