**United States of America**
**Federal Trade Commission**

**Remarks at the Global Antitrust Institute**

# FTC vs. Facebook

**Christine S. Wilson***
**Commissioner, U.S. Federal Trade Commission**

**Antonin Scalia Law School**
**Arlington, VA**
**December 11, 2019**

* The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner. Many thanks to my Attorney Advisor, Robin Rosen Spector, for assisting in the preparation of these remarks.

Good afternoon. Thank you to Professor Joshua Wright and the Global Antitrust Institute for providing the venue and refreshments for this event. It is a pleasure to be back at this wonderful institution. I also want to acknowledge the George Mason law students who have briefly set aside their outlines and casebooks as the end of the semester approaches. Thank you for breaking away from cramming for finals to come for the caffeine (or sugar) and stay for the speech!

As will become clear, the comments I make today are my views only and do not reflect the views of the Federal Trade Commission or any other Commissioner.

I have been a Commissioner for just over a year. Many of the matters I review are clear-cut, making the decision process quite straightforward. Other cases – Qualcomm on the antitrust side and Facebook on the consumer protection side – are far more complex. These are the cases that literally have kept me awake at night, grappling with how best to advance the interests of American consumers. These cases require nuanced and objective analysis, and benefit from a thoughtful and measured approach to the legal and policy issues presented.

During the course of the Facebook investigation, I spent a great deal of time reviewing evidence, posing questions to staff, consulting with my fellow Commissioners, and cross-examining the company. There were many decisions to make along the way – which counts to include in the complaint? What relief will provide an appropriate deterrent effect? Should we pursue individual liability? Should we prolong the investigation by seeking further discovery? Should we litigate or negotiate a settlement? How do we handle violations that inevitably will come to light after this matter is concluded? In the end, though, the most important question for

me came down to this: How can we most effectively lay the foundation for a culture of compliance at Facebook and best protect the public in the future?

I have counseled hundreds of clients in numerous different industries during my legal career. Unlike my fellow commissioners, I have also served as in-house counsel, an experience that gives me even greater insight into the complexities of compliance initiatives. My clients have ranged from small, privately held companies to publicly traded Fortune 10 companies. They have made products and offered services as widely varied as prescription drugs and air travel. Each one has had unique and distinctive goals and corporate imperatives.

In my decades of practice, though, I have discovered one universal phenomenon that transcends all of these apparent differences: A culture of compliance must begin with the top executives, or it will fail. I have learned through experience, sometimes hard won, that it is not enough for a general counsel to urge his business counterparts to follow the law. A truly compliant company arises because the CEO or the President tells his or her employees that each person in the company will follow the law in all that he or she does – and then devotes the resources and the time to achieving that goal. In other words, the message needs to come from the very top, that the company will <u>both</u> talk the talk and walk the walk.

Today, my goal is to explain why I believe the FTC settlement with Facebook was the most effective way to ensure that Facebook takes it privacy obligations seriously and adopts a culture of compliance. My discussion today will cover three topics. First, I will explain how Facebook violated the law and how staff recommended that we address the violations. Second, I will explain why I voted to accept the settlement. Third, I will discuss why the early signs validate this choice and why this settlement is an appropriate exercise of the Commission's authority.

## I. Facebook's Conduct and Staff's Recommendation

### A. Facebook's Law Violations

As you may know, this settlement was not Facebook's first rodeo with the FTC. In 2012, the FTC charged Facebook with eight separate privacy violations including deceptive claims about consumers' ability to control the privacy of their personal data. The FTC and Facebook reached a settlement that: (1) prohibited misrepresentations about the privacy and security of consumer information, (2) prohibited misrepresentations regarding Facebook's sharing of data, (3) required Facebook to implement a comprehensive privacy program, and (4) required Facebook to obtain assessments of its privacy program from a qualified third party.

Unfortunately, Facebook repeatedly violated the 2012 order. As alleged in the FTC's July 2019 complaint, Facebook again misrepresented how consumers could control the privacy of their data and the manner and extent to which it shared consumers' data.

Specifically, we allege that Facebook told consumers that, through the privacy settings, they could limit how their information would be shared – for example, with friends. But Facebook failed to clearly disclose to consumers that it would share their data with app developers for apps that the consumer's friends used. Thus, apps acquired troves of data about Facebook users without consumers' knowledge or consent.

Here is how this amassing of data worked. Facebook user A limits her information to friends in the privacy settings and is friends with user B. User B takes a quiz on an app and consents to that app having access to his data. The quiz gets access to user B's data and the data of all of user B's friends, including user A. This transmission of information goes on behind the scenes without a clear disclosure to consumers and in flagrant disregard of consumers' privacy choices. And this is the practice that allowed Cambridge Analytica to cause so much harm.

Importantly, as we allege, Facebook knew that apps were gaining access to vast amounts of data. As our complaint explains, when Facebook conducted an audit of its apps it found that over a 30-day period, the apps were making hundreds of millions of requests for friend data. One app made 450 million requests in 30 day period! These requests were 33 times the number of this app's monthly active users.

After news of Cambridge Analytica broke, the FTC immediately began investigating and made the rare decision to confirm the investigation. We uncovered these misrepresentations about data sharing as well as numerous other violations that showed a pattern of misrepresentations and a culture of putting profits before privacy.

For example, our complaint alleges that in April 2015, Facebook announced publicly at a conference that it was terminating third-party apps' ability to access friend data. Despite this announcement, Facebook maintained private arrangements with dozens of companies – which it called "White Listed Apps." These arrangements gave these apps continued access to the friend data. Our complaint alleges that Facebook awarded White List status based on considerations of advertising and other revenues.

In another example challenged in our complaint, Facebook told consumers they would collect their phone numbers only for security purposes. Contrary to its representations, Facebook also used the phone numbers for advertising purposes.

Similarly, in April 2018, our complaint alleges that Facebook told users they must opt-in to use facial recognition for user-uploaded photos or videos. But tens of millions of users actually had to opt-out to disable the facial recognition.

Our investigation also found that Facebook did not screen or vet apps adequately to assess and address privacy risks posed by the apps on Facebook. Given the vast amounts of data Facebook was allowing apps to access, the privacy risks were significant.

As this investigation proceeded, my fellow Commissioners and I received regular updates from the staff. It became clear to me that this company lived its motto – move fast and break things. As a disruptive start-up, that may be a good thing. But when a company manages the data of 2.2 billion people around the world, a different approach is required. I explained to staff that we needed to extract relief that would require Facebook to slow down, assess the impact of its actions on consumer privacy, and act accordingly. While we cannot force a company to adopt a culture of compliance, we can impose systems that provide oversight and accountability.

B. The Negotiated Settlement

The Facebook settlement that staff negotiated includes unprecedented and record-breaking relief. It has three significant components – conduct provisions that fundamentally change Facebook's privacy ecosystem, a $5 billion civil penalty, and other injunctive relief addressing data security and specific misrepresentations.

The privacy provisions are the cornerstone of the relief. This order imposes a robust and multi-layered system of checks and balances that extinguishes CEO Mark Zuckerberg's ability unilaterally to chart the path for handling consumer data at Facebook. The layered privacy program requires assessments of privacy risks, creates accountability to the CEO and the Board of Directors, and imposes oversight from the Board, a third-party assessor, and the FTC.

The order vests the day-to-day implementation of the privacy program with the business personnel who must conduct privacy risk reviews and document material privacy decisions. The order mandates heightened protection for certain categories of products and services, including

those directed at minors. Designated Compliance Officers (DCOs), appointed by an independent privacy committee on the Board, supervise this process.

The order further requires that decisions regarding these privacy risks be documented and transmitted to Mr. Zuckerberg and the Board of Directors so that knowledge, responsibility, and accountability for privacy decisions is dispersed throughout the organization. The order then obligates Mr. Zuckerberg (and the Chief Privacy Officer), with the knowledge gained through this process, to certify quarterly, on pain of civil and even criminal penalties, that Facebook's privacy program is in compliance with the law.

The order also requires creation of a new independent privacy subcommittee whose members are to be appointed by an independent nominating committee. The nominating committee must ensure that members have appropriate qualifications to serve; Facebook officers and employees, including CEO Zuckerberg, cannot be members. This committee also reviews the privacy documentation produced at the business level and meets quarterly to receive briefings from management and the outside assessor. In addition, the committee must consult with outside privacy experts. We included this provision to ensure that Facebook does not exist in its own echo chamber on privacy issues but instead seeks the input of external experts who will offer objective guidance on privacy best practices.

Finally, the order empowers an independent third-party assessor with the tools and authority needed to assess and monitor compliance with the order, and to throw caution flags that alert the Board of Directors and the FTC when necessary. Under this order, we have greater access to information and authority over the assessor, including the power to approve and remove the assessor.

The order's corporate governance requirements were designed to incentivize compliance and institutionalize accountability. For example, the certification provisions are modeled after Sarbanes-Oxley. I observed first hand while in private practice that when an executive must sign a certification it focuses the mind. This phenomenon is widely acknowledged. In testimony describing the impact of the Sarbanes-Oxley Act in driving compliance with the new regime, the Securities and Exchange Commission has stated that "the certification provisions have perhaps had the greatest immediate impact."[1] Rational executives in the shoes of Mr. Zuckerberg and the Facebook Chief Privacy Officer will be incentivized to focus very carefully on the substance of their obligations.

The order also takes into account the fact that a board needs both independence and a flow of information to exercise effective oversight.[2] The governance provisions in this Facebook order include both. The privacy committee receives reports and updates from management, meets quarterly to discuss privacy issues and with the independent assessor without management present. The members of the Board, as in any publicly traded company, have fiduciary obligations to the shareholders and potential liability for failing to live up to their obligations.

While the privacy provisions constitute the heart of the order, the settlement also includes a record civil penalty of $5 billion. This penalty dwarfs all previous privacy fines both nationally and globally – it is roughly 200 times the largest U.S. privacy penalty and 20 times greater than the largest European fine assessed or imposed. The only time the U.S. government

---

[1] Chairman William H. Donaldson, Testimony Concerning the Impact of the Sarbanes-Oxley Act, Before the House Committee on Financial Services (April 21, 2005), https://www.sec.gov/news/testimony/ts042105whd.htm. The Chairman further explained that "the Act affirms senior executive responsibility for the financial reporting process of public companies by requiring CEOs and CFOs to certify the financial reporting process and other information in their reports filed with the Commission."

[2] Jill Fisch, *The New Federal Regulation of Corporate Governance*, 28 Harvard J Law & Pub. Pol'y 39, 43-44 (2004).

has obtained a larger penalty occurred with respect to Deepwater Horizon, an environmental disaster that contaminated the Gulf of Mexico, killed countless and precious forms of wildlife, and destroyed people's livelihoods. This penalty also establishes a new benchmark for FTC challenges to privacy violations in the future.

This penalty is based on sound legal and economic analysis. The Commission's determination of an appropriate civil penalty in any matter is a multi-faceted analysis that uses the five factors prescribed by courts – the good or bad faith of the defendants; injury to the public; the desire to eliminate the benefits derived from the violations; the defendant's ability to pay; and the necessity of vindicating the Commission's authority.[3]

I cannot disclose our deliberative process or non-public information but I can say that our Bureau of Economics (BE) conducted a careful analysis of the benefits derived by the violations and the injury incurred by the public. BE routinely considers economic literature that addresses the harm to consumers from alleged violations in FTC matters. BE analysis evaluates the number of consumers affected, the conduct, the law violations, and the harm from those violations. Where the matter involves an order violation, in addition to the estimate of harm, the penalty typically includes an appropriate multiplier to ensure that the relief effectively vindicates the Commission's authority. The analysis presented to me in this matter was robust and sound, and the civil penalty that we imposed comports with BE's analysis.

And, finally, the additional injunctive relief in this order is unprecedented. In addition to the comprehensive privacy program requirements I just outlined, the order addresses protection

[3] *See, e.g., United States v. Danube Carpet Mills*, 737 F.2d 988, 993 (11th Cir. 1984) (noting that the following factors should be assessed in setting a civil penalty amount: "(1) the good or bad faith of the defendants; (2) the injury to the public; (3) the defendants' ability to pay; (4) the desire to eliminate the benefits derived by the violations; and (5) the necessity of vindicating the authority of the FTC" (citing *United States v. Reader's Digest Ass'n*, 662 F.2d 955, 967 & n. 18 (3d Cir. 1981); *United States v. J.B. Williams Co.*, 498 F.2d 414, 438-39 (2d Cir. 1974))); *accord United States v. Alpine Indust., Inc.*, 352 F.3d 1017 (6th Cir. 2003).

for phone numbers, and facial recognition. This is also the only FTC order to require both a comprehensive privacy program and a comprehensive data security program. The order also includes requirements for data breaches[4] and requires that Facebook delete the data from users who terminate their accounts.

## II. My Review

When presented with the draft settlement, I considered very carefully whether it was the most effective way to prompt Facebook to confront its failings and adopt a constructive approach to consumer data. I could not vote for a settlement unless it met my goal of fostering a culture of compliance. I reviewed the staff's recommended settlement through that lens. I pored over every detail of the proposed order and worked closely with staff to extract additional important relief. The civil penalty amount was not determinative for me. Although I believe the penalty will serve as a deterrent for both Facebook and other companies that handle consumer data, the conduct relief was my primary focus.

I worked with staff, my colleagues, and Facebook to refine the order provisions until I was convinced that the order provided the structure necessary to incentivize compliance. As modified following additional negotiations, I believe that the robust and layered privacy program this order imposes represents a sea change in the way Facebook must conduct its privacy and data security program. The settlement also provides strong and certain relief for consumers immediately, and establishes a roadmap for other companies regarding the FTC's expectations with respect to how consumer data should be handled. While I understand the benefits of litigation that my dissenting colleagues sought, including transparency, the remarkable package

[4] Facebook is obligated to create incident reports that it must deliver to the Commission that describe how the breach was remediated, and must continue providing reports every 30 days until the incident is fully investigated and resolved.

of relief we obtained in this settlement is clearly superior to the potential benefits of litigation that we might have obtained far in the future.

III. Order Has and Will Have an Impact and Is An Appropriate Use of FTC Authority

Early signs validate that adopting this settlement was the best way to advance the public interest. First, the settlement has had immediate effects on Facebook. When we announced the settlement, Mark Zuckerberg stated "[w]e've agreed to pay a historic fine, but even more important, we're going to make some major structural changes to how we build products and run this company. . . . We expect it will take hundreds of engineers and more than a thousand people across our company to do this important work."[5] Although the judge has not yet entered the order, Facebook has started implementing it.

In November, Facebook's new Chief Privacy Officer stated that the settlement has been a "catalyst for new systems of accountability."[6] Our enforcement division has been receiving regular updates from Facebook that indicate an appropriate trajectory. Facebook is implementing a substantially strengthened, time and resource-intensive privacy review process for all new products and features (including any changes to existing products and features) prior to launch. A thorough retrospective review has uncovered unauthorized data access by apps, leading Facebook to announce that it suspended tens of thousands of apps.[7] In addition to reviewing data risks, Facebook is embedding restrictions on the sharing of user data within its programming. Facebook has undertaken a comprehensive review of its code to reshape and

[5] Mark Zuckerberg, *Statement* (July 24, 2019), https://www.facebook.com/zuck/posts/10108276550917411.

[6] Chon, Gina, *Cost of business*, Breakingviews, Nov. 22, 2019, https://www.breakingviews.com/considered-view/facebook-should-keep-the-confessions-coming/.

[7] Facebook Blog Post: *An Update on Our App Developer Investigation* (Sept. 20, 2019), https://about.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/.

control how information is flowing through its systems and tightening controls to ensure that Facebook is not solely relying on written policies and manual review to catch issues. Facebook also has launched features for consumers to see the data that businesses have compiled about them and allow them to delete or disassociate that data.[8] While I cannot vouch for the representations that Facebook has made, I can say that the company appears to be appropriately focused on fulfilling its obligations under the order.

Second, the industry has taken notice. FTC privacy orders set the standards for industry and this order in particular is reverberating through the industry. Approximately a month after the FTC announced the Facebook settlement, I was on the West Coast for a privacy conference and met with Silicon Valley executives. They peppered me with questions about the obligations imposed on Facebook pursuant to the order and whether to accord with best practices their companies should consider building in various governance safeguards. To be clear, my answer was "it depends." The structure of Facebook, the types of data it collects, and the fact that the settlement was a resolution of order violations contributed to the relief extracted there. These types of processes and governance measure might not be necessary for every company to be in compliance with the law.

Another meeting I had with industry, just prior to the announcement of the Facebook order, also demonstrates how FTC orders affect other firms in the same industry. In February 2019, the FTC reached a settlement with TikTok resolving allegations that the site violated the Children's Online Privacy Protection Act (COPPA).[9] A company called Yoti that provides tools

[8] Chon, Gina, *Cost of business*, Breakingviews, Nov. 22, 2019, https://www.breakingviews.com/considered-view/facebook-should-keep-the-confessions-coming/.

[9] *U.S. v. Musical.ly*, No. 2:19-cv-01439 (C.D. Cal. Feb. 27, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc.

to assist companies in obtaining verifiable parental consent, as required by COPPA, saw a marked increase in their business following the announcement of the TikTok settlement. They attribute this increase directly to our enforcement action.[10] In other words, other players in this space, seeing the TikTok order, are getting their own houses in order. Why? To avoid being the target of FTC enforcement. This outcome provided yet another data point for a phenomenon I know to be true: When the FTC acts, similarly situated companies take notice and re-evaluate their own conduct. FTC orders have both specific and general deterrent effects.

The reactions of privacy groups to Facebook order are also instructive. The Centre for Information Policy Leadership (CIPL) released a white paper in November discussing the implications of the FTC settlements in Facebook and Equifax. CIPL explicitly acknowledged that "FTC consent orders have precedential value beyond the target of an investigation."[11] The paper explains that the privacy program requirements outlined in the recent FTC settlements address all elements of organizational accountability. CIPL conducted a detailed mapping of the Facebook settlement against the General Data Protection Regulation (GDPR) and concluded that the order substantially aligns with GDPR in many ways but goes beyond GDPR in several significant areas, including the order's certification provisions.[12] CIPL concluded that the

[10] *See* Statement of Chairman Joe Simons and Commissioner Wilson Regarding YouTube (Sept. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1542922/simons_wilson_google_youtube_statement.pdf (footnote 5 and Attachment A).

[11] Organizational Accountability in Light of FTC Consent Orders, Centre for Information Policy Leadership (Nov. 13, 2019), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_organizational_accountability_in_light_of_ftc_consent_orders__13_november_2019_.pdf.

[12] *Id.* at 7-12. For example, the certification provision in the Facebook order requires more than GDPR certifications provisions. GDPR certifications require specific processing obligations, whereas the Facebook certifications must cover the organization's management program. The certification provisions by covered third parties in the Facebook order – the apps – also exceed those required by GDPR, which does not require due diligence on data sharing partners or mandate how third party due diligence must be undertaken. GDPR also does not require setting up an independent privacy committee. Neither does it require an independent assessor or the extensive reporting

Facebook (and Equifax) settlements include the "essential elements of accountability and also potentially increase, in meaningful ways, the baseline expectations for any organization's accountability program."[13]

Academics also have long observed the effects of FTC privacy orders on industry. For example, Daniel Solove, a law professor at the George Washington University Law School, has explained that FTC settlements have created a common law of privacy. "[C]ompanies look to these agreements to guide their privacy practices. Thus, in practice FTC privacy jurisprudence has become the broadest most influential regulating force on information privacy in the United States – more so than nearly any privacy statute or any common law tort."[14]

It is important to pause and acknowledge that the FTC extracted this far-reaching, unprecedented conduct relief using a 100 year old statute designed long before the invention of television, let alone the smart phone and the Internet. Any relief we hypothetically could have achieved in litigation would need to be tied to the violations of the order or Section 5 of the FTC Act, which prohibits deceptive and unfair practices.

I had the honor of serving with Chairman Muris when the FTC's first privacy and data security cases, Eli Lilly & Microsoft, were brought. These initial FTC privacy cases used our deception authority to challenge misrepresentations in privacy policies.[15] The FTC's privacy

---

and recordkeeping requirements in the Facebook order. Finally, GDPR does not mandate enforcement of company platform terms against independent third parties, which is a requirement of the Facebook order.

[13] *Id.* at 15.

[14] Daniel J. Solove and Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Columbia L. Rev. 583 (2014).

[15] In the Matter of Eli Lilly, C-4047 (2002), https://www.ftc.gov/enforcement/cases-proceedings/012-3214/eli-lilly-company-matter; In the Matter of Microsoft Corporation, C-4069 (2002), https://www.ftc.gov/enforcement/cases-proceedings/012-3240/microsoft-corporation-matter. In Eli Lilly, the company disclosed that consumers were using Prozac despite representations in its privacy policy that it would protect consumer privacy. We challenged this statement as deceptive under Section 5. The Microsoft case was primarily a data security case but the case also

program has evolved and developed considerably since then. The relief in this order builds on that body of work but is tied to the deceptive privacy and order violation allegations in the complaint – as legally it must be. I recognize that there are many other concerns that have been raised about Facebook, including allegations of monopolization, biased treatment of content, and unfair involvement in elections. Those issues fall outside the scope of this privacy and data security enforcement action and remain unresolved.

Critics of the Facebook settlement, including two of my colleagues, lament that we did not do more. For example, they sought more limitations on Facebook's data collection and use. Commissioner Chopra in particular stresses that our settlement did nothing to change the company's business model, its structure, or its financial incentives. But, Facebook's business model under the current legal framework, is not unlawful.

I recognize that consumers are concerned, and some even deeply troubled, by the ways in which Facebook (and other companies in the United States) collect, aggregate, and monetize data. I share concerns about many of the data collection and monetization practices that seem ubiquitous in this era.

But an action to enforce the terms of an FTC order is not an appropriate vehicle to set standards for how Facebook, and by extension all other platforms and companies in the United States, collect, use, aggregate, share, sell, and otherwise monetize data. The FTC historically has been chastised by the courts – and Congress – for overstepping its bounds. In the 1970s, the FTC's aggressive intervention led detractors to call it "the second most powerful legislature" in

---

challenged representations in the privacy policy on use of data. The FTC has also has used its unfairness authority, particularly in data security, to challenge security practices that provide injury to consumers not outweighed by countervailing benefits to consumers and competition. *See, e.g.,* In the Matter of Lenovo, Inc. No. 1523134 (Sept. 2017), https://www.ftc.gov/system/files/documents/cases/1523134_c4636_lenovo_united_states_complaint.pdf; FTC v. D-Link Corp., et al., No. 3:17-CV-39-JD (N.D. Cal 2017), https://www.ftc.gov/enforcement/cases-proceedings/132-3157/d-link.

America.[16] Recognizing the limits of the FTC's authority, we understand that decisions about what data can be collected and how it can be used and monetized appropriately fall within the purview of Congress.

To address these issues, we need baseline federal privacy legislation. I was extremely pleased to see that last week, the Senate Commerce Committee held a hearing on privacy legislation. Senators Wicker and Cantwell have both introduced privacy bills, and I appreciate their leadership on this important issue. I do hope that, even in this tumultuous period, Congress is able to reach a consensus and act on this important issue. In the interim, the FTC will use its current authority vigorously to protect consumer privacy. The Facebook settlement is an excellent example of how the FTC has deployed that authority appropriately and responsibly to impose relief that will have a profound impact on not only Facebook but all companies that collect consumer data. I am confident that my decision to vote to accept the settlement was correct.

Thank you again to Professor Wright and GAI for hosting this event. I am happy to take questions now.

[16] See, e.g., J. Howard Beales III & Timothy J. Muris, FTC Consumer Protection at 100: 1970s Redux or Protecting Markets to Protect Consumers?, 83 Geo. Wash. L. Rev. 2157, 2159 (2015) (quoting Jean Carper, The Backlash at the FTC, Wash. Post, Feb. 6, 1977, at C1).