



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

**Statement of Chairman Joe Simons
and Commissioners Noah Joshua Phillips and Christine S. Wilson
In re Facebook, Inc.
July 24, 2019**

The Order announced today resolving the FTC’s investigation of Facebook is an historic victory for American consumers. The record-breaking penalty and unprecedented, sweeping conduct relief serves the public interest and far exceeds what the Commission could expect to receive at the end of litigation years from now.

In 2012, Facebook entered into a consent order with the FTC, resolving allegations that the company misrepresented to consumers the extent of data sharing with third-party applications and the control consumers had over that sharing. The 2012 order barred such misrepresentations, and required Facebook to establish a reasonable program to protect privacy. Our complaint announced today alleges that Facebook failed to live up to its commitments under that order. Facebook subsequently made similar misrepresentations about sharing consumer data with third-party apps and giving users control over that sharing, and misrepresented steps certain consumers needed to take to control facial recognition technology. Facebook also allowed financial considerations to affect decisions about how it would enforce its platform policies against third-party users of data, in violation of its obligation under the 2012 order to maintain a reasonable privacy program. In addition to these order violations, today’s complaint alleges that Facebook violated the FTC Act by engaging in a new set of deceptive practices relating to the collection and use of consumer phone numbers provided by consumers to enable security features such as two-factor authentication.

The Commission’s career enforcement staff conducted an extremely thorough investigation for over a year that focused on all potential violations of the FTC’s 2012 order and Section 5 of the FTC Act. The sweeping settlement announced today is based on the staff’s recommendation, and includes three major components: a record-breaking \$5 billion penalty; new substantive privacy and data security requirements; and significant structural reforms to ensure greater corporate accountability, more rigorous compliance monitoring, and increased transparency.

I. Facebook is Subject to a Record-Breaking \$5 Billion Penalty

The \$5 billion penalty serves as an important deterrent to future order violations, by Facebook and others. Five billion dollars is approximately 9% of Facebook’s 2018 revenue, and approximately 23% of its 2018 profit. For purposes of comparison, the EU’s General Data Protection Regulation (GDPR) is touted as the high-water mark for comprehensive privacy

legislation, and the penalty the Commission has negotiated is *over 20 times greater* than the largest GDPR fine to date. This penalty is also one of the largest civil penalties in U.S. history—alongside only cases involving enormous environmental damage and massive financial fraud. The magnitude of this penalty resets the baseline for privacy cases—including for any future violation by Facebook—and sends a strong message to every company in America that collects consumers’ data: where the FTC has the authority to seek penalties, it will use that authority aggressively.

II. The Order Imposes Significant New Privacy and Data Security Obligations on Facebook

The Order imposes significant new privacy obligations on Facebook. For example, it requires greater oversight of third-party developers, including a requirement to terminate developers’ access to users’ information if they fail to certify that they are in compliance with Facebook’s platform policies or fail to justify their need for specific user data. Facebook must also enforce its platform terms against app developers solely on the basis of the severity of the violation and without regard to the financial benefit that flows to Facebook from the relationship. Pursuant to the Order, Facebook must expand its existing privacy program to cover WhatsApp and any Facebook product or service that receives personal information from Facebook or WhatsApp. (Instagram, as a part of Facebook, is also covered by the Order.) Moreover, this is the first FTC order to address biometric information, requiring Facebook to get consumers’ opt-in consent before using or sharing such information in ways that exceed prior disclosures and consents. In addition to requiring a comprehensive privacy program, the Order also requires Facebook to establish and maintain a comprehensive data security program, a combination of obligations not imposed by any other FTC order. The Order also specifies data security obligations related to authentication, access controls, and encryption. Collectively, these requirements will not only alter the way Facebook does business, but also send an important signal to the marketplace about privacy and security best practices.

III. The Order Imposes a Sea Change in the Way Facebook Addresses Compliance with its Privacy Obligations

Finally, the Order imposes a privacy regime that includes a new corporate governance structure, with corporate and individual accountability and more rigorous compliance monitoring. The new privacy regime requires several different mandatory information flows about privacy decisions through multiple internal and external channels of compliance, so that if there is breakdown in one or more channels, another channel can identify the problem and fix it. This approach dramatically increases the likelihood that Facebook will be compliant with the Order; if there are any deviations, they likely will be detected and remedied quickly.

Five Channels of Compliance to Hold Facebook Accountable

The Order’s five overlapping channels of compliance are as follows. First, Facebook must establish a new Board of Directors committee focused solely on privacy-related risks and Order compliance, which creates greater accountability at the Board level. Members of the privacy committee must be independent directors with relevant privacy and corporate

compliance expertise, and will be appointed by a nominating committee comprised of independent directors. Privacy committee members are also protected from removal by the controlling shareholder under a revised corporate charter: members may not be removed for reasons relating to their good-faith actions as privacy committee members, absent an affirmative vote by two-thirds of the voting shares (more than the votes Mark Zuckerberg controls). The privacy committee must discuss with Facebook management the company's privacy risks and the steps the company intends to take to monitor or mitigate such risks. The privacy committee must also discuss privacy risks with the independent third-party assessor, both with and without management present.

Second and third, Mark Zuckerberg and the Designated Compliance Officers (DCOs) independently must submit to the Commission quarterly certifications that the company is in compliance with the privacy program mandated by the Order, as well as an annual certification that the company is in overall compliance with the Order. Thus, the Order requires accountability at the individual level. False certifications would subject Mr. Zuckerberg and the DCOs to personal liability, including civil and criminal penalties.¹

Fourth and fifth, the Order strengthens external oversight of Facebook by giving new tools to an independent third-party assessor and to the FTC to monitor Facebook going forward. Both the assessor and the FTC will have access to Facebook's documentation of its privacy decisions, including quarterly privacy review reports and the incident reports required by the Order. Importantly, the Order also enhances the assessor's responsibilities, subjects the assessor to evaluation by the independent privacy committee, and gives the FTC the ability both to approve and to terminate the assessor if he or she fails to carry out these responsibilities thoroughly. Additionally, the FTC will now have the full panoply of discovery tools provided by the Federal Rules of Civil Procedure to monitor Facebook's compliance and investigate non-compliance.

Transparency to Ensure Meaningful Oversight

To ensure that Facebook executives, the Board, the assessor, and the FTC can exercise meaningful oversight, the Order creates an unprecedented level of transparency for Facebook's privacy practices by mandating four different information flows. The first information flow is mandated by the Order's privacy program, which requires Facebook to assess and address the privacy risks associated with each new or modified product, service, or practice *before* it is implemented, and document assessments in privacy review statements. The Order requires Facebook to implement safeguards to address identified privacy risks and document in these privacy review statements alternative safeguards that would mitigate those risks, but were not implemented. The DCOs must integrate these statements into a quarterly privacy review report, which the DCOs then provide to the CEO and the assessor, and upon request, to the Commission. Relevant personnel charged with implementing the privacy program must also sub-certify that the company has implemented each requirement of the program.

¹ See 18 U.S.C. § 1001.

The second information flow consists of incident reports documenting when data of 500 or more users has been compromised, which Facebook must deliver to the Commission and the assessor within 30 days of the company's discovery of the incident, together with a description of the steps taken to remediate the issue. Facebook must continue to provide reports every 30 days until the incident is fully investigated and resolved.

The third information flow consists of the independent assessor's biennial assessments of Facebook's privacy program, which must be based primarily on the assessor's independent fact-gathering, sampling, and testing. The assessor will submit the assessments to the Commission. The assessor must also provide the biennial assessment to the independent privacy committee, and must meet with the privacy committee to discuss both Order compliance and any problems with Facebook management.

The fourth information flow consists of Facebook management and the assessor briefing the privacy committee at regularly-scheduled meetings. Each quarter, the privacy committee must receive a briefing from Facebook management regarding the state of Facebook's privacy program, Facebook's compliance with the Order, and material risks to the privacy of users' information. As for the assessor, the reporting is not limited solely to the formal biennial reports. At least quarterly, the privacy committee must meet with the assessor, without Facebook management present, to discuss the assessor's ongoing assessment of Facebook's privacy program and any privacy risks the assessor has identified. The privacy committee must review with Facebook management any proposed remediation plans to address issues raised by the assessor.

These information flows will help the privacy committee assess whether the privacy program is in compliance with the Order, allow the assessor to perform a more meaningful assessment, permit the DCOs and CEO to make informed certifications, and enable the FTC to promptly investigate potential instances of noncompliance. There is no guarantee that Facebook will not have further privacy missteps. But these multiple information flows to individuals and entities responsible for holding the company accountable will provide both a constant reminder of the company's privacy obligations as well as overlapping oversight, which together increase the likelihood that someone inside or outside the company will identify a problem and sound the alarm. If Facebook violates the Order, then the Commission can argue that a penalty even greater than \$5 billion is warranted and that the public interest can only be served via additional monetary and injunctive relief.

IV. The Settlement Far Exceeds What Could be Achieved in Litigation and Gives Consumers Meaningful Protections Now

Put simply, today's settlement is unprecedented, both in terms of the magnitude of the civil penalty and the scope of the conduct relief. To reach this result, the Commission started and ended its analysis in pursuit of one goal above all: to obtain the most meaningful relief to best protect the American public. Whether to settle or litigate, and whether to label an individual a "defendant" or not, are potential means to attain this goal—not goals in and of themselves. To evaluate whether we would accomplish our goal, we asked: "Is the relief we would obtain through this settlement equal to or better than what we could reasonably obtain through

litigation?” If the answer had been “no,” it would have made sense to aggressively move forward in court. The answer, however, was “yes”—because the relief we have secured today is substantially greater than what we realistically might have obtained by litigating, likely for years, in court.² Moreover, a settlement brings immediate changes to Facebook’s flawed privacy and data security practices and requires immediate protections for Facebook users. In light of our responsibility to be effective stewards of the public resources entrusted to the Commission, it would not have made sense to pursue protracted and expensive litigation likely to yield substantially weaker relief.

The \$5 billion penalty assessed against Facebook today is orders of magnitude greater than in any other privacy case, and also represents almost double the greatest percentage of profits a court has ever awarded as a penalty in an FTC case. If the FTC had litigated this case, it is highly unlikely that any judge would have imposed a civil penalty even remotely close to this one. Even assuming the FTC would have eventually prevailed on liability, the court would not automatically impose the maximum penalty permissible under Section 5(l) of the FTC Act.³ Rather, courts enjoy a great deal of discretion in assessing civil penalties under the FTC Act,⁴ and they often depart, dramatically and downwardly, from the theoretical maximum. For example, the highest civil penalty a court has awarded in a litigated FTC consumer protection case was in *United States v. Dish Network, LLC* for violations of the Telemarketing Sales Rule.⁵ After finding that Dish was culpable and had engaged in “years and years of careless and reckless conduct,” the court awarded \$168 million in civil penalties, even though the maximum theoretical penalty was over \$727 billion.⁶ The civil penalty imposed represented 12% of Dish’s profits at the time. The government has only obtained civil penalties of billions of dollars in rare cases involving environmental disasters or large-scale financial fraud.⁷

² Judged by any reasonable metric—financial impact, changes to Facebook governance, privacy requirements on the company—there is no convincing argument that litigation would have achieved more.

³ 15 U.S.C. § 45(l).

⁴ When determining the amount of a civil penalty for *order* violations, the factors delineated in *United States v. Reader’s Digest Ass’n, Inc.*, 662 F.2d 955 (3d Cir. 1981), have become standard considerations by the court: defendant’s good or bad faith, injury to the public, defendant’s ability to pay, elimination of the benefits of a violation, and the necessity of vindicating the authority of the FTC. The FTC Act directs the court to consider similar factors when determining the amount of a civil penalty for a *rule* violation: the defendant’s degree of culpability, history of prior conduct, ability to pay, ability to continue to do business, and other matters as justice may require. 15 U.S.C. § 45(m)(1)(C).

⁵ *United States v. Dish Network, LLC*, 256 F. Supp. 3d 810 (C.D. Ill. 2017).

⁶ *Id.* at 970, 983.

⁷ Department of Justice (“DOJ”) Press Release, *Bank of America to Pay \$16.65 Billion in Historic Justice Department Settlement for Financial Fraud Leading up to and During the Financial Crisis* (Aug. 21, 2014), <https://www.justice.gov/opa/pr/bank-america-pay-1665-billion-historic-justice-department-settlement-financial-fraud-leading> (\$5 billion civil penalty to settle DOJ claims under the Financial Institutions Reform, Recovery and Enforcement Act); DOJ Press Release, *U.S. and Five Gulf States Reach Historic Settlement with BP to Resolve Civil Lawsuit Over Deepwater Horizon Oil Spill* (Oct. 5, 2015), <https://www.justice.gov/opa/pr/us-and-five-gulf-states-reach-historic-settlement-bp-resolve-civil-lawsuit-over-deepwater> (\$5.5 billion civil penalty to settle DOJ claims under the Clean Water Act).

And that is just the money. The Order’s innovative, far-reaching conduct relief—imposing affirmative obligations and corporate governance reforms—extends well beyond the typical relief historically awarded by the courts in consumer protection cases involving legitimate companies. Even assuming the FTC would prevail in litigation, a court would not give the Commission carte blanche to reorganize Facebook’s governance structures and business operations as we deem fit. Instead, the court would impose the relief. Such relief would be limited to injunctive relief to remedy the specific proven violations and to prevent similar or related violations from occurring in the future.⁸ Thus, it is highly unlikely the Commission could have obtained this magnitude of injunctive relief if we had proceeded with litigation. For example, because we do not, and could not, allege and prove that Facebook’s current Board structure is illegal or that changes in corporate governance are necessary to effectuate compliance with the Order and the FTC Act, it is unlikely that a court would mandate any corporate governance reforms.

Our colleagues lament that the Order does not do more. For example, they would rather the Order impose more limitations on data collection and use. The argument that “more is better” is certainly appealing, but it relies on a false dichotomy: a hypothetical “more” versus the extraordinary and certain relief the Commission has obtained. As a civil law enforcement agency (and not a regulator), we can only get what we can win in litigation⁹ or via hard-fought negotiations. The FTC does not have the authority to regulate by fiat. The extent to which Facebook, or any other company, should be able to collect, use, aggregate, and monetize data, is something Congress should evaluate in its consideration of federal privacy legislation. Our 100-year-old statute does not give us free rein to impose these restrictions. In order to serve the public interest and provide real protections for consumers, the Commission must compare settlement options against what it might reasonably obtain through litigation. Viewed through this lens, today’s Order is a complete home run. Litigation would have delayed the imposition of these important consumer protections and, in all likelihood, would have led to reduced deterrence and weaker privacy protections. Despite this reality, two of our colleagues dissent—meaning they would prefer that we pursue lengthy and uncertain litigation instead of implementing relief that will start protecting consumers immediately.

V. Mark Zuckerberg is Being Held Accountable and the Order Cabins His Authority

Our dissenting colleagues argue that the Commission should not have settled because the Commission’s investigation provides an inadequate basis for the decision not to name Mark Zuckerberg personally as a defendant. This criticism misses the mark because it focuses on optics over substance. The provisions of this Order extinguish the ability of Mr. Zuckerberg to make privacy decisions unilaterally by also vesting responsibility and accountability for those decisions within business units, DCOs, and the privacy committee. That said, Mr. Zuckerberg

⁸ See, e.g., *DOJ v. Daniel Chapter One*, 89 F. Supp. 3d 132, 143 (D.D.C. 2015), *aff’d*, 650 F. App’x 20 (D.C. Cir. 2016); *FTC v. John Beck Amazing Profits LLC*, 888 F. Supp. 2d 1006, 1011-12 (C.D. Cal. 2012), *aff’d*, 644 F. App’x 709 (9th Cir. 2016).

⁹ As noted previously, even if the Commission were to succeed at litigation, the types of conduct prohibited or required by a court are constrained by the allegations laid out in the complaint and proven in litigation and what the court considers to be reasonable “fencing-in” relief.

will be held accountable for certifying quarterly—under threat of civil and criminal penalties—that the company’s privacy program is in compliance with the Order. The relief we have achieved today solves concrete problems, rather than venting frustration with individuals.

In addition, our colleagues argue that the Order is ineffective because it does not remove *all* of Mr. Zuckerberg’s power to control Facebook’s Board of Directors. But the Order significantly diminishes Mr. Zuckerberg’s power—something no government agency, anywhere in the world, has thus far accomplished. The Order requires multiple information flows and imposes a robust system of checks and balances relating to Order compliance, making it much harder for Mr. Zuckerberg to steamroll the company into disregarding users’ privacy, were that his goal, or claim plausible deniability about the company’s privacy practices. It is also worth repeating that we must compare this relief to what we might achieve by litigating the case. It is unrealistic to think that court-imposed relief would remove Mr. Zuckerberg as CEO of Facebook or strip him of substantial voting rights.

VI. The Commission Retains Full Authority to Enforce Compliance with a New Stricter Order and Section 5 of the FTC Act

Our colleagues also object to the settlement based on their belief that the release in this matter is too broad, leaving the Commission unable to sue based on any future revelations about Facebook’s past conduct. The Order releases all claims for 2012 order violations prior to June 12, 2019, and for consumer protection Section 5 claims *known* by the FTC prior to June 12, 2019. Releases are a practical reality of settlements and are used as bargaining chips during negotiations to extract the desired relief from a defendant. Many Department of Justice and other federal agency settlements (including other FTC settlements) have, in exchange for the appropriate relief, released a company, and its officers and directors, from liability for all conduct alleged (and similar conduct) under the law applicable to those situations.¹⁰ Our

¹⁰ See, e.g., Agreement for Compromise Settlement and Release, *United States v. Barclays Capital, Inc.*, No. 16-CV-7057(KAM/JO) (E.D.N.Y. Apr. 24, 2018), ECF No. 137, <https://www.justice.gov/opa/press-release/file/1047101/download> (releasing Barclays and two officers from all claims that were or could have been asserted in the action, as well as any other civil claim under certain statutes and common law theories for conduct alleged in the complaint and conduct more broadly related to other residential mortgage-backed securities deals); Stipulation and Order of Settlement and Dismissal with Prejudice, *United States v. Wells Fargo Bank, N.A.*, No. 12CIV7527JMFJCF (S.D.N.Y. Apr. 8, 2016), ECF No. 320, <https://www.justice.gov/opa/file/839796/download> (releasing Wells Fargo, and its officers and directors, from any civil or administrative monetary claim under certain statutes and common law theories for conduct alleged in the complaint and conduct relating to single-family residential FHA loans).

Commissioner Chopra points out that the Department of Justice’s *Justice Manual*, which serves as policy guidance for Department prosecutors, advises that with respect to civil cases, “where the Department reaches a resolution with a company before resolving matters with responsible individuals, Department attorneys should take care to preserve the ability to pursue the individuals.” DOJ, *Justice Manual, Compromising and Closing, 4-3.100 – Pursuit of Claims Against Individuals*, <https://www.justice.gov/jm/jm-4-3000-compromising-and-closing#4-3.100>. However, Commissioner Chopra fails to point out that this guidance is not presented in absolute terms and is dependent on whether further action against individuals is “necessary or warranted to service the public interest.” *Id.* (“The Department should preserve the ability to pursue civil remedies against those individuals, *unless further action is not necessary or warranted to serve the public interest.*” (emphasis added)). Here, we have made the determination that, in light of the meaningful relief we have achieved, retaining the ability to sue Mr. Zuckerberg for past order violations we did not find and for which he may have been personally liable would not serve the public interest.

yearlong investigation,¹¹ which uncovered a substantial number of violations, leaves us comfortable that the extraordinary relief obtained in this case is more than adequate to remedy any as-yet-unknown violation of the 2012 order. In addition, all potential Section 5 and 2012 order violations the Commission currently knows about are addressed in this Order—we are not giving Facebook a pass on any order violations staff has uncovered. Because the release preserves all *unknown* Section 5 claims, the release does not bar the Commission from bringing a claim for a Section 5 violation it did not know about prior to this Order. Our primary goal, again, is to establish safeguards to protect consumers. We would rather do that now, not years from now. Any ongoing or future conduct remains subject to prosecution under both Section 5 and, maybe even more importantly, the new stricter Order.

VII. Conclusion

We are extremely proud of the landmark penalty and conduct relief announced today. The size of the \$5 billion penalty, as well as the percentage of profits it represents, will provide significant deterrence not just to Facebook, but to every other company that collects or uses consumer data. This penalty raises the bar for civil penalties in future matters involving privacy violations. Moreover, the Commission designed the Order's sweeping injunctive relief not only to punish future violations, but more importantly to implement dramatic privacy transparency and oversight changes at Facebook, thereby decreasing the likelihood that those violations will occur in the first place. We are confident that any evaluation of the Order based on its merits and a rational understanding of the law will yield but one conclusion: this settlement represents an unprecedented victory for consumer privacy.

¹¹ Staff made dozens of investigative demands, following up on each, often multiple times. Staff also investigated numerous issues that arose during the course of the investigation, including those raised in news reports and various complaints filed by consumer groups. The allegations we make and the relief we secured regarding facial recognition, for example, stem from an inquiry initiated following relevant news reports and a complaint by a consumer group. See, e.g., Jessica Guynn, *Facebook wants to save your face. Should you say yes to facial recognition?*, USA TODAY (Apr. 19, 2018), <https://www.usatoday.com/story/tech/news/2018/04/19/facebook-growing-use-facial-recognition-raises-privacy-concerns/526937002/>; Katie McInnis, *Complaint to the FTC Regarding Facebook's Face Recognition Setting*, CONSUMER REPORTS ADVOCACY (May 20, 2019), <https://advocacy.consumerreports.org/wp-content/uploads/2019/05/Complaint-to-FTC-Consumer-Reports-May-2019-2.pdf>. Staff reviewed millions of pages of documents and hundreds of pages of interrogatory responses. Moreover, staff coordinated with and received information from our law enforcement partners.