UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA

In re Facebook, Inc.
Commission File No. 1823109

July 24, 2019

Executive Summary

- **Facebook's violations were a direct result of the company's behavioral advertising business model.** Facebook flagrantly violated the FTC's 2012 order by deceiving its users and allowing pay-for-play data harvesting by developers. The company's behavioral advertising business, which monetizes user behavior through mass surveillance, contributed to these violations. Cambridge Analytica's tactics of profiling and targeting users were a small-scale reflection of Facebook's own practices.

- **The proposed settlement does little to change the business model or practices that led to the recidivism.** The settlement imposes no meaningful changes to the company's structure or financial incentives, which led to these violations. Nor does it include any restrictions on the company's mass surveillance or advertising tactics. Instead, the order allows Facebook to decide for itself how much information it can harvest from users and what it can do with that information, as long as it creates a paper trail.

- **The $5 billion penalty is less than Facebook's exposure from its illegal conduct, given its financial gains.** These illegal data practices were tools to lock in and advance the company's digital advertising dominance. The FTC can seek civil penalties in addition to unjust gains. The Commissioners supporting this settlement do not cite any analysis of Facebook's unjust enrichment to justify the proposed $5 billion payment, and I believe the company's potential exposure is likely far greater. In the Commission's 2012 action against Google, the FTC obtained a penalty of more than five times the company's unjust gains. This is a departure from that approach.

- **The proposed settlement lets Facebook off the hook for unspecified violations.** The settlement gives Facebook a legal shield of unusual breadth, deviating from standard FTC practice. Given the many public reports of problems at Facebook, it is hard to know how wide the range of conduct left unaddressed in the proposed Complaint or settlement may be. This shield is good for Facebook, but leaves the public in the dark as to how the company violated the law, and what violations, if any, are not remedied.

- **The grant of immunity for Facebook's officers and directors is a giveaway.** 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. The Commissioners supporting this settlement do not point to any documents or sworn testimony to justify this immunity.

- **The case against Facebook is about more than just privacy – it is also about the power to control and manipulate.** Global regulators and policymakers need to confront the dangers associated with mass surveillance and the resulting ability to control and influence us. The behavioral advertising business incentives of technology platforms spur practices that are dividing our society. The harm from this conduct is immeasurable, and regulators and policymakers must confront it.

I. Introduction: Facebook and its Role in Society

In March 2018, news reports revealed that Cambridge Analytica, a political consulting firm, had harvested data from millions of Facebook users by baiting people with a personality quiz. The firm was hired by others to target messaging to prospective U.S. voters based on psychological profiles developed through this data. After the revelations, the Federal Trade Commission[1] formally opened an investigation into Facebook's privacy practices, which were already subject to a law enforcement order.

In many ways, Cambridge Analytica's scheme was a small-scale reflection of Facebook's own tactics of tricking users into sharing excessive amounts of personal data and then getting paid by third parties to target individual users. Cambridge Analytica wouldn't have had all the personal information it had if Facebook didn't collect it. They wouldn't have been able to use the information to manipulate users if Facebook didn't facilitate it.

The Cambridge Analytica scandal and the others that followed force us to confront the role of Facebook in society. Facebook's founder and Chief Executive Officer Mark Zuckerberg said early on that the company's goal is to "move fast and break things." It certainly has. We are continually learning how fake news, election interference, incitement of violence, discrimination, and other serious harms can trace their way back to Facebook.

Facebook is not a government. Facebook is a private, for-profit corporation, and we should reasonably assume it seeks to advance its own financial gains. Here, Facebook's behavioral advertising business model is both the company's profit engine and arguably the root cause of its widespread and systemic problems. Behavioral advertising generates profits by turning users into products, their activity into assets, their communities into targets, and social media platforms into weapons of mass manipulation. We need to recognize the dangerous threat that this business model can pose to our democracy and economy.

I believe behavioral advertising incentivizes many of Facebook's most concerning practices. It works by using people's past behavior to predict and place the ads most likely to influence their future behavior. The more Facebook knows about a user, the more it can accurately determine which ads will successfully achieve the advertiser's desired outcome.

This thirst for data has led the company to harvest intimate, personal details about tens of millions of Americans on a scale and scope that are almost unimaginable. Facebook's data collection is both ongoing and increasing, as the company continues to add new means of surveillance that can be difficult to avoid. To facilitate further data acquisition, Facebook grants itself the right to surveil, own, and monetize users' private information by binding them to constantly evolving take-it-or-leave-it terms at sign-on.

[1] Throughout this document, references to the Federal Trade Commission ("FTC" or "Commission") denote only the deliberative body of five Commissioners, not the agency's staff, unless otherwise specified. Legal authority to compel documents and testimony, file lawsuits, and refer matters to the Department of Justice is vested in the Commission. In this matter and others, the agency's staff skillfully execute upon the direction of the Commissioners, and the Commissioners are ultimately accountable for those decisions.

Because behavioral advertising allows advertisers to use mass surveillance as a means to their undisclosed and potentially nefarious ends, Facebook users are exposed to propaganda, manipulation, discrimination, and other harms. In a sales pitch for its digital advertising, Facebook boasts that its advanced targeting is better than the limited options offered by other platforms because "people on Facebook share their true identities, interests, life events and more."[2] Facebook's massive, private, and generally unsupervised network of advertisers has virtually free rein to microtarget its ads based on every aspect of a user's profile and activity. The company's detailed dossiers of private information includes things like a user's location and personal connections, but it also includes the history of everything a user has ever done wherever Facebook is embedded in the digital world.

Advertisers use this personal information to craft messages designed to appeal to a user's tastes and beliefs. The flood of hyper-targeted advertising influences the company's secret algorithms that shape and prioritize each user's content feed in undisclosed, opaque ways. This kind of individual message tailoring can carry real-world risks when wielded with ill intent. It can be used to encourage and incite offline behavior, and shape understanding of the world and belief systems in ways that affect communities and countries. Yet Facebook's advertising model allows almost anyone to pay for access to this powerful tool.

Little is known about Facebook's mysterious methods for setting advertising prices and reporting ad engagement metrics. What we do know is that because behavioral advertising monetizes every action a user takes, Facebook places a premium on the engagement that keeps people active on the platform. Facebook can reward engaging ads by promoting them, even if they are from malicious actors seeking to manipulate and sow seeds of division and discontent. It does all of this while invoking legal immunity under Section 230 of the Communications Decency Act[3] as a shield against any fallout from the problematic content users are exposed to on Facebook's platform.

The FTC has a long history of enforcement against advertising practices that deceive and manipulate by design. In 2015, the agency published a strong enforcement policy statement on deceptively formatted advertisements.[4] Given the FTC's expertise in deceptive advertising, ascertaining Facebook's compliance is a prerequisite for addressing potential manipulation.

---

[2] *Your Guide to Digital Advertising*, FACEBOOK BUSINESS https://www.facebook.com/business/help/1029863103720320?helpref=page_content (last visited July 22, 2019).

[3] Pub. L. No. 104-104 § 230, 110 Stat. 56 (1996).

[4] *See Enforcement Policy Statement on Deceptively Formatted Advertisements* (Dec. 22, 2015), https://www.ftc.gov/public-statements/2015/12/commission-enforcement-policy-statement-deceptively-formatted. That statement clearly stated that "regardless of the medium in which an advertising or promotional message is disseminated, deception occurs when consumers acting reasonably under the circumstances are misled about its nature or source, and such misleading impression is likely to affect their decisions or conduct regarding the advertised product or the advertising." *Id*. at 2. It further notes that "over the years, the Commission staff have addressed the potential for consumers to be deceived by various categories of advertising formats, such as ads appearing in a news or feature story format, deceptive endorsements, undisclosed sponsorship of advertising and promotional messages, and ads in search results." *Id*. at 2-3.

The FTC's 2015 policy statement includes a discussion of native advertising and notes that "the recent proliferation of natively formatted advertising in digital media has raised questions about whether these advertising formats deceive consumers by blurring the distinction between advertising and non-commercial content." *Id.* at 10. For

I was one of the earliest users of Facebook, then called thefacebook.com, in its opening days of operation. Facebook's violations of law have harmed democracy and society. Now, the company seeks to further integrate across its empire and launch a global currency. Whether our democracy is prepared for this onslaught is a question that should concern everyone in our society.[5]

Breaking the law has to be riskier than following it. As enforcers, we must recognize that until we address Facebook's core financial incentives for risking our personal privacy and national security, we will not be able to prevent these problems from happening again.

I dissent from the Federal Trade Commission's proposed settlement, entered by the Attorney General and subject to further approval by a federal court. The settlement's $5 billion penalty makes for a good headline, but the terms and conditions, including blanket immunity for Facebook executives and no real restraints on Facebook's business model, do not fix the core problems that led to these violations.

II. Background and Overview of Investigation and Violations

A. Facebook and Mark Zuckerberg

Fifteen years ago, Mark Zuckerberg launched Facebook. The company's offering served as a way for college students to communicate in a closed network where users could control the dissemination of information. Facebook expanded to additional college campuses, and over time, added other affiliations where users could connect with one another, such as sharing a common workplace. Facebook would soon be open to any user. Facebook has made many acquisitions, including the photo-sharing platform Instagram and messaging platform WhatsApp.

In 2012, Facebook went public (NASDAQ: FB). Despite being a public company, Mark Zuckerberg retains unusual control over the firm, given his stake in a class of shares with special voting rights. Zuckerberg is also Chairman of the Board of Directors. He and Chief Operating Officer Sheryl Sandberg serve simultaneously as executive officers and voting board members.

In its history, the company has been the subject of a number of controversies, and Facebook's practices have often been at the epicenter of debates about the future of the internet and the role of digital platforms.

B. The 2011 Complaint and 2012 Final Order

---

instance, "if a natively formatted ad appearing as a news story is inserted into the content stream of a publisher site that customarily offers news and feature articles, reasonable consumers are unlikely to recognize it as an ad." *Id.* at 12. The statement further notes that "the target audience of an ad also may affect whether it is likely to mislead reasonable consumers about its nature or source. Increasingly, in digital media, advertisers can target natively formatted ads to individual consumers and even tailor the ads' messaging to appeal to the known preferences of those consumers." *Id*.

[5] For further discussion on the impact of surveillance on society and the economy, s*ee, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (PublicAffairs, 1st ed. 2019).

Today's settlement is not the first time that Facebook has been the subject of an enforcement action by the FTC. In 2011, the FTC filed an eight-count complaint against Facebook after conducting an investigation into the company's privacy practices. The complaint focused on Facebook's deception, specifically, its representations about how it shares and protects user data.

The Commission charged Facebook with a host of violations related to privacy and data collection.[6] The net effect of all these violations was to induce users into handing over more data that Facebook could share with developers and third parties.

For example, Facebook changed its website so certain information that users may have designated as private, like their Friends List, was made public without their approval. Facebook even made representations that third-party apps would have access only to user information that they needed to operate. In reality, the apps could access nearly all of users' personal data.

Facebook promised users that it would not share their personal information with advertisers. That wasn't true. Facebook also claimed that when users quit the platform, their photos and videos would be inaccessible. But that wasn't true either.

In lieu of taking a case to trial, the Commission voted to resolve the matter through a settlement. Facebook and the FTC voluntarily entered into an order that, among other things:

- Barred Facebook from making misrepresentations about the privacy or security of users' personal information;
- Required Facebook to obtain users' affirmative express consent before enacting changes that override their privacy preferences; and
- Required Facebook to establish and maintain a comprehensive privacy program designed to address privacy risks associated with the development and management of new and existing products and services, and to protect the privacy and confidentiality of consumers' information.

The order also required independent assessments by a third party every two years to determine whether Facebook's practices met or exceeded the requirements of the order. Separately, the order also gave the Commission broad access to documents to ensure Facebook was in compliance.

C. Overview of 2018 Investigation and Summary of Violations Alleged in New Complaint

After the 2012 order was finalized, there were ongoing concerns about Facebook's commitment to compliance. In addition, Facebook's business model continued to evolve, as the company engaged in more acquisitions and began ingesting more categories of data. In March 2018, after news broke about Cambridge Analytica, the FTC announced that it had opened an investigation

[6] Press Release, FTC, Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

into Facebook's privacy practices. In the months that followed, there was a steady stream of additional public reports regarding potential privacy and security lapses by Facebook.

As Commission staff undertook an investigation, I requested periodic briefings on the status and any findings or conclusions. Based on the material presented to me, I was very concerned about Facebook's cooperation and candor in its dealings with the Commission and its staff. In my view, there were multiple inconsistencies and deficiencies in Facebook's responses to questions. I questioned whether the company's document productions were truly complete. I believe that Facebook struggled to answer many requests for data, and I ascertained that the company was resistant to providing documents from Zuckerberg's files.

It became clear to me that the agency would have limited visibility into the full range of potential violations of the 2012 order, as well as potential violations of law that fell outside the scope of the order. Nonetheless, despite what I see as our limited visibility into key aspects of the company's conduct, the Commission and its staff found strong evidence that Facebook violated the terms of the 2012 order, including:

Flagrant deception regarding user control.[7] Millions of American users relied on Facebook's deceptive settings and statements to restrict the sharing of their information to their Facebook "friends," when, in fact, third-party developers could still access and collect their data. There were material misrepresentations throughout Facebook's user settings and privacy tools.

Facebook knew or should have known that this conduct violated the 2012 order because it was engaging in the very same conduct that led to the filing of the original legal action.

Massive conflicts of interest with favored advertisers and partners.[8] In 2014, Facebook and its CEO publicly announced that Facebook would stop allowing third-party developers to access data from the "friends" of app users.[9] But unbeknownst to users, Facebook allowed "grandfathered" developers already on the platform – including the developer that would later harvest voter information on behalf of Cambridge Analytica[10] – to continue collecting data on the "friends" of its users for at least another year.[11] Certain favored developers continued this collection well into 2018.[12]

Facebook not only left gaps in its privacy policies but also enforced those policies unevenly depending on how much revenue third parties were generating for the company. Internal documents noted that Facebook would allow apps spending more than a certain threshold on advertising to collect excessive user information, while Facebook would terminate access to apps spending less than that threshold.[13] This selective enforcement and other related conduct were clear violations of the order.

[7] Facebook Compl. ¶¶ 39-58.
[8] Facebook Compl. ¶¶ 8-13.
[9] Facebook Compl. ¶¶ 7, 111-113.
[10] Kogan Compl. ¶¶ 12-13.
[11] Facebook Compl. ¶¶ 116-117.
[12] Facebook Compl. ¶ 8.
[13] Facebook Compl. ¶¶ 103-106.

The investigation also uncovered additional violations, including false assurances to users that they would need to opt in to facial recognition.[14] In addition, Facebook encouraged users to turn over their phone numbers for security purposes, but used those phone numbers to feed the company's surveillance and advertising business.[15]

Notably, these serious failures took place even as PriceWaterhouseCoopers, the "independent third party" retained pursuant to the 2012 order, was evaluating Facebook's privacy policies for compliance. While third-party assessments can provide valuable information, the incentives of these private, for-profit overseers may not always be well aligned.[16]

D. Order Enforcement

FTC orders are not suggestions. When the Commission believes that facts warrant formal enforcement action or an amendment to the existing order, it has a number of options at its disposal that are not limited to the Commission's chosen course in this matter.[17]

- Refunds to Consumers and Forfeiture of Ill-Gotten Gains. The Federal Trade Commission can seek equitable relief from a federal court under Section 13(b) of the FTC Act.[18] Equitable relief can take many forms. For example, if anything of value was taken from consumers, this value can be refunded or redressed. Similarly, if a company was able to generate revenue or profits through its illegal acts, the FTC can seek the forfeiture of these gains. Both remedies are commonly pursued and do not require the involvement of the Department of Justice ("DOJ").
- New Order with Tougher Restrictions. Commission Rule 3.72(b)[19] allows the Commission to issue an Order to Show Cause as to why a firm's current order should not be reopened and amended. Firms can respond to the order and avail themselves of a hearing. After such time, the Commission can issue a new order, which can impose additional restrictions on the firm, including, for example, limits on the collection, sharing, and use of personal information. The Commission does not need to go to federal court under this procedure, though parties can appeal the Commission's final order to a circuit court of appeals.
- Civil Penalties. The Commission can also pursue a civil penalty action against violators of agency orders. The agency must refer the matter to the DOJ, and the Attorney General can then file a complaint seeking civil penalties of up to $42,530 per violation from a court.

[14] Facebook Compl. ¶¶ 150-160.
[15] Facebook Compl. ¶¶ 161-176.
[16] Third-party compliance monitors frequently lack independence from the firms they are paid to monitor, which can reduce their effectiveness. I have raised similar concerns in the context of our COPPA Safe Harbor program. *See Prepared Remarks of Comm'r Rohit Chopra at the Common Sense Media Truth about Tech Conference*, FED. TRADE COMM'N (Apr. 4, 2019), https://www.ftc.gov/system/files/documents/public_statements/1512078/chopra_-_truth_about_tech_4-4-19.pdf.
[17] The Commission has tools available to pursue more than one of these avenues, and in fact, the Commission's proposed resolution contemplates both a stipulated federal order and a revised administrative order.
[18] 15 U.S.C. § 53(b).
[19] 16 C.F.R. § 3.72(b).

III. Root Causes of Facebook's Order Violations

The FTC Act does not require a showing of ill intent to establish liability, but uncovering the motivations of individuals or firms believed to have broken the law is essential when crafting effective injunctive relief that protects the public from further harm.

Facebook is a large, sophisticated company under a formal agency order. I do not believe its serious violations of that order were merely inadvertent or technical in nature. Instead, the evidence suggests that these violations were clearly motivated by Facebook's financial incentives.

A. Facebook's Profit Model is Propelled by Surveillance and Manipulation

When we think of surveillance, we often think of debates regarding the appropriate limits of surveillance by the state, where proponents and opponents argue about safety and civil liberties. When the entity engaged in mass surveillance is a corporation, we face similar issues, but without public accountability. It is becoming increasingly clear that companies like Facebook also rely on mass surveillance of users. For a private, profit-maximizing firm, this raises serious concerns about incentives.

In 2018, Facebook had revenues of $55.8 billion, the bulk of which came from "advertisers" rather than paid services or software licensing. Facebook does not sell a traditional advertising product; it sells user behavior. Like other companies engaged in online behavioral advertising, Facebook monetizes the actions of users, in addition to passive observation of a display advertisement. Facebook makes more money when users engage in an action, such as clicking on specific content. To maximize the probability of inducing profitable user engagement, Facebook has a strong incentive to (a) increase the total time a user engages with the platform and (b) curate an environment that goads users into monetizable actions.

To accomplish both of these objectives, Facebook and other companies with a similar business model have developed an unquenchable thirst for more and more data. This data goes far beyond information that users believe they are providing, such as their alma mater, their friends, and entertainers they like. Facebook can develop a detailed, intimate portrait of each user that is constantly being updated in real time, including our viewing behavior, our reactions to certain types of content, and our activities across the digital sphere where Facebook's technology is embedded. The company can make more profit if it can manipulate us into constant engagement and specific actions aligned with its monetization goals.

As long as advertisers are willing to pay a high price for users to consume specific content, companies like Facebook have an incentive to curate content in ways that affect our psychological state and real-time preferences. For example, if Facebook's algorithms detect more engagement when users are sad or angry, then the company has an incentive to present content in ways that make users feel sad or angry. Even when companies like Facebook dispute that they are engaging in activities akin to mass surveillance or manipulation, their business incentives strongly motivate them to do so and their technology enables it, regardless of whether or not it is a deliberate business decision.

B. Facebook Needed to Show Progress to Wall Street on Mobile and Third-Party Developers

For years, Facebook and Mark Zuckerberg had eschewed making the move to becoming a publicly traded firm. Around the time that the FTC filed its initial complaint in 2011, news reports suggested that Facebook was approaching five hundred investors,[20] which triggers public financial reporting under the securities laws.

On February 1, 2012, Facebook filed its intent with the Securities and Exchange Commission to move forward with an initial public offering. As part of preparations to become a public company, Facebook and Zuckerberg conducted "roadshows" to potential investors, a common practice prior to an initial public offering. A core part of the pitch to investors was Facebook's plans to become a major player in the mobile environment.[21]

Soon after Facebook went public, it was reported that Mark Zuckerberg was frustrated with the company's mobile strategy, and a key plank of his turnaround plan was to attract app developers[22] – in part by ensuring they could monetize user engagement.[23] Finding ways to attract and maintain lucrative relationships with developers was a key priority for the company's top leadership during that period, including Zuckerberg himself.[24] In fact, it was reported that during this time, any decision to ban an app "required the personal approval" of Zuckerberg. No matter what a developer was up to, its access to the data was protected unless Zuckerberg himself signed off.[25]

These relationships with developers proved immensely valuable to Facebook. Partnerships with apps drove user engagement, which drove advertising, and reciprocity agreements with these apps meant that the company could augment its data collection further still.

Facebook's order violations fueled this cycle. Within months of the FTC's order being finalized – and not long after its initial public offering – Facebook reconfigured its privacy policy to hide from users how to opt out of sharing with third parties.[26] The number of users this targeted was

---

[20] Steven Davidoff Solomon, *FTC and the 500-Person Threshold*, N.Y. TIMES: DEALBOOK (Jan. 3, 2011, 4:03 PM), https://dealbook.nytimes.com/2011/01/03/facebook-and-the-500-person-threshold/.
[21] Alistair Barr, *Facebook's Zuckerberg Says Mobile First Priority*, REUTERS (May 11, 2012, 10:02 PM), https://www.reuters.com/article/net-us-facebook-roadshow/facebooks-zuckerberg-says-mobile-first-priority-idUSBRE84A18520120512.
[22] Kurt Wagner, *Inside Facebook's Mobile Strategy*, MASHABLE (Sept. 20, 2013), https://mashable.com/2013/09/20/facebook-mobile-strategy/.
[23] Sarah Perez, *Facebook's Platform Mission: Help You Build, Grow, and Monetize*, TECHCRUNCH (Sept. 11, 2013), https://techcrunch.com/2013/09/11/facebooks-platform-mission-help-you-build-grow-and-monetize/.
[24] *See* Selected Documents Ordered from Six4Three, Ex. 170 (FB-01156203) https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf (revealing discussions by Mark Zuckerberg and other senior executives on how to increase revenue and data collection from app developers).
[25] Paul Lewis, *'Utterly Horrifying': Ex-Facebook Insider Says Covert Data Harvesting Was Routine*, THE GUARDIAN (Mar. 20, 2018, 7:46 AM), https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.
[26] Facebook Compl. ¶¶ 44-58.

potentially vast – academic studies suggest that as many as 75 percent of users were interested in further restricting their privacy settings.[27] If they had done so it would have significantly reduced the platform's attractiveness to developers, and the company's attractiveness to shareholders. Facebook and its CEO knew that many of its users were confused, but persisted with these practices long after promising to halt them.[28]

Breaking the law likely yielded other benefits for Facebook, too. Its selective enforcement of platform policies rewarded its most lucrative developers. Tricking users into turning over their phone numbers improved the company's ad targeting.[29] Deceiving users about its facial recognition practices made it harder for them to turn off surveillance.

Ultimately, Facebook abused the public's trust because advertisers and developers – not Facebook's users – are its core constituency. It is telling that even as Facebook marketed users' social graphs to third-party developers, the company did not allow users themselves to access the same information through the "Download my Data" feature, making it more difficult for users to leave the platform.[30] The public learned that games like Farmville and apps such as the one feeding Cambridge Analytica could see your social graph, but you could not access your own.

IV. Role of Officers and Directors in Facebook's Order Violations

"I started Facebook, I run it, and I'm responsible for what happens here."
- Mark Zuckerberg

Corporate executive officers and directors serving on corporate boards play a critical role in ensuring compliance with applicable law and regulation. This is particularly important when a corporation becomes subject to an administrative agency order.

---

[27] This is merely an estimate, but is one supported by a number of studies. In one study, 75% of posts from a sample of users had settings other than "public," while fewer than half of study participants had multiple privacy settings across posts. *See* Casey Fiesler et al., *What (or Who) Is Public? Privacy Settings and Social Media Content Sharing*, PROCEEDINGS OF THE 2017 ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK AND SOCIAL COMPUTING (CSCW '17) (2017), www.tandem.gatech.edu/wp-content/uploads/2016/10/cscw2017_FacebookPrivacy.pdf. According to a second study, by early 2010, 79% of users had changed their privacy settings to tighter controls, indicating widespread user interest in stepping up privacy protections. *See* Deirdre O'Brien & Ann M. Torres, *Social Networking and Online Privacy: Facebook Users' Perceptions*, 31(2) IRISH J. OF MGMT. 63, 63–97 (2012), https://aran.library.nuigalway.ie/handle/10379/4059. Finally, in a 2018 survey, 74% of Facebook users reported that they adjusted their FB usage in the twelve months prior to June 2018, by either not using Facebook for an extended period, adjusting privacy settings, or deleting the FB app. *See* Andrew Perrin, *Americans are Changing Their Relationship with Facebook*, PEW RESEARCH CENTER (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

[28] In a 2014 address, Mark Zuckerberg explained, "we've also heard that sometimes you can be surprised when one of your friends shares some of your data with an app. . . . So now we're going to change this, and we're going to make it so that now, everyone has to choose to share their own data with an app themselves. . . . [W]e think this is a really important step for giving people power and control over how they share their data with apps." In fact, Facebook continued allowing favored developers to harvest friend data. *See* Facebook Compl. ¶¶ 112-117.

[29] Kashmir Hill, *Facebook Is Giving Advertisers Access to Your Shadow Contact Information*, GIZMODO (Sept. 26, 2018, 3:40 PM), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051.

[30] *See* Josh Constine, *Facebook shouldn't block you from finding friends on competitors*, TECHCRUNCH (2018), https://techcrunch.com/2018/04/13/free-the-social-graph/.

Two individuals simultaneously serve as executive officers and members of Facebook's board of directors: Mark Zuckerberg and Sheryl Sandberg. Zuckerberg is the Founder, Chief Executive Officer, and Chairman of the Board of Directors of Facebook. Sandberg is the Chief Operating Officer and is a member of the Board of Directors of Facebook.

A. Officers and Directors Are Bound by Agency Orders and Can Be Liable for Order Violations

FTC orders bind both the named corporation and its officers and directors, regardless of whether they are named individually.[31] And officers and directors cannot avoid responsibility under these orders simply by burying their heads in the sand as their subordinates break the law. Instead, they are bound "… to take all reasonable steps to effect compliance."[32] Failure to do so can expose them to liability for wrongdoing.[33]

There are good reasons the law imposes this heightened obligation. Were it not to, "we would be putting a premium on ignorance and offering a sanctuary for those remiss in performing their duties as corporate officers…"[34] Moreover, through active participation in prohibited activity or through willful blindness toward others' misconduct, corporate executives can often enjoy significant financial gains from violating an order. Failing to hold them accountable only encourages other officers to be similarly neglectful in discharging their legal obligations.

In my view, it is appropriate to charge officers and directors personally when there is reason to believe that they have meaningfully participated in unlawful conduct, or negligently turned a blind eye toward their subordinates doing the same. There is precedent for the FTC not only charging individuals officers with order violations but also holding them personally liable for civil penalties, even when they were not named in the original order.[35] This is a reasonable approach that should not be limited to cases involving smaller firms.

B. Investigating the Role of Individuals is Critical in Cases Involving Order Violations

Because the law imposes affirmative obligations on officers and directors whose firms are under order, uncovering their role in potential violations is critical to any investigation. It is especially critical in this investigation, which involved a firm that is tightly controlled by its founder, CEO, and Chairman, Mark Zuckerberg. Given the structure of his ownership and his special voting rights, it is hard to imagine that any of the core decisions at issue were made without his input. Whether Zuckerberg took all reasonable steps to ensure compliance with the 2012 order is an essential determination we should evaluate carefully before pursuing any resolution, including,

---

[31] *See* Fed. R. Civ. P. ("Rule") 65(d). Rule 65(d) "is equally germane to orders enforcing decisions of administrative agencies." *Reich v. Sea Sprite Boat Co., Inc.*, 50 F.3d 413, 417 (7th Cir. 1995).
[32] *U.S. v. Greyhound*, 363 F. Supp. 525, 572 (N.D. Ill. 1973), *supplemented*, 370 F. Supp. 881 (N.D. Ill. 1974), and *aff'd*, 508 F.2d 529 (7th Cir. 1974) (holding individual corporate officers liable for order violations).
[33] *Id*.
[34] *Id*. (quoting *In re Dolcin Corp.*, 247 F.2d 524 (D.C. Cir. 1956)).
[35] *See, e.g., U.S. v. Budget Marketing, Inc.*, No. 88-1698-E (S.D. Iowa, Mar. 17, 1997) (consent decree imposing penalties on individuals officers); *U.S. v. SMI/USA, Inc.*, No. 3:94-CV-0058-T (N.D. Tex. Oct. 25, 1993) (same).

for example, by thoroughly reviewing documents in his custody and examining him under oath.[36]

In fact, in their discussion of the investigation and proposed settlement, the Commissioners supporting this outcome do not cite a single deposition[37] of Zuckerberg or any other Facebook officer or director. The FTC Act does not include special exemptions for executives of the world's largest corporations, but this settlement sends the unfortunate message that they are subject to another set of rules.

V. Proposed Settlement Fails to Remedy Core Problems and Prevent Future Harm

A. The Settlement Places No Substantive Restrictions on Facebook's Data Collection Practices

The proposed order places no meaningful restrictions on Facebook's ability to collect, share, and use personal information. Instead, the order allows Facebook to evaluate for itself what level of user privacy is appropriate, and holds the company accountable only for producing those evaluations. What it does not require is actually respecting user privacy.

The Privacy Program mandated by the order[38] includes two core provisions: First, it requires that Facebook design processes to protect against privacy risks posed by third-party developers. Second, it requires that Facebook design processes to protect against privacy risks posed by the company's new products, practices, or services.[39] But these provisions are less than meets the eye. When reviewed carefully, it becomes apparent that Facebook is essentially allowed to decide for itself the extent to which it will protect user privacy.

As to third-party developers, the order requires that Facebook a) obtain a certification from every developer verifying compliance with platform terms and justifying data collection; b) cut off developers that fail to justify their data collection; c) conduct reviews to ensure developers' compliance with platform terms; and d) enforce platform terms reasonably.[40]

But these safeguards are flimsy, as they provide no limitation or even guidance on what constitutes justified information collection. As a result, it is highly unlikely this will affect the

---

[36] As discussed further below, I believe there is already sufficient evidence, including through public statements, to support a charge against Mark Zuckerberg for violating the 2012 order. But in a case as complex as this one, we cannot fully understand his role in the order violations – and how to prevent future violations – without a more complete investigation.

[37] This is known as an "investigational hearing" when conducted before litigation.

[38] *United States v. Facebook*, _____ Attachment A to the Proposed Federal Court Order, Administrative Decision and Order, Part VII.

[39] Separately, the order includes consent restrictions on third-party sharing, heightened consent requirements for facial surveillance of certain users, information deletion requirements, limitations on the use of telephone numbers, employee access restrictions, and restrictions on password security. These provisions are meaningful, but do not meaningfully constrain the company. The third-party sharing consent restrictions are largely identical to those imposed in 2012, and the other restrictions target discrete privacy or security lapses rather than imposing bright line rules on information harvesting.

[40] *Id.* Part VII.E.1.

quantity or nature of information that developers collect, so long as their lawyers can adequately state a justification.

The restrictions placed on new products, practices, and services are similarly narrow. The order essentially states that if a new product or service is deemed to pose a "material risk" to user privacy, the company must prepare a Privacy Review Statement describing a) what information is being collected and why; b) how users will be notified about the information collection; c) whether users will need to consent to the information collection; d) any risks to user information; e) how the company plans to mitigate those risks; and f) alternative ways to mitigate risks that the company is not pursuing.[41]

These requirements do not actually place any substantive limit on Facebook's collection, use, or sharing of personal information. For example, this subsection explicitly applies to "the sharing of Covered Information with a Facebook-owned affiliate." Given Facebook's intent to integrate Messenger, WhatsApp, and Instagram, the procedures required by the order are a good proxy for the extent to which the order constrains Facebook generally.

The order does not prohibit the integration of the platforms; it requires only that Facebook designate the integration as a potential user risk. It does not require users to consent to the integration; it requires only that Facebook describe its consent procedures, "if any." It does not limit what constitutes an acceptable level of risk to users; it requires only that the risks be documented. It does not require that Facebook eliminate or even minimize these risks; it requires only that it describe a process for mitigating them.

There are few limits on Facebook's discretion around these issues. While the order requires the designation of Compliance Officers[42] and the appointment of an Assessor[43] and an Independent Privacy Committee,[44] their power is largely limited to ensuring compliance with the narrow procedural requirements described above.

The Designated Compliance Officers design the Privacy Program, summarize Privacy Review Statements for the CEO, and sign certifications. But rather than charging the Officers with achieving any benchmarks – e.g. minimizing collection, minimizing sharing, or minimizing user risk – they are charged only with ensuring that paperwork has been completed.

Similarly, the Independent Assessor is charged with ensuring that the Privacy Program is effective, but is given no benchmarks for what constitutes effectiveness. While the Independent Assessor can potentially prod Facebook to make changes around disclosures or consent procedures, it is unlikely to be able to stop a major program change, such as the platform integration described above, so long as Facebook can adequately state a justification for the change.

[41] *Id.* Part VII.E.2.
[42] *Id.* Part VII.C.
[43] *Id.* Part VIII.
[44] *Id.* Part X.

The powers of the Independent Privacy Committee appear to be even more limited. The Committee is charged with receiving briefings on the Privacy Program and the assessments, but is not given any specific authority over the design, budget, or management of the Privacy Program. (As detailed further below, the composition of the Committee can be heavily influenced by the CEO.)

Finally, the requirement for certifications by the CEO is laudable, but limited. He is required only to certify that the procedural boxes listed above have been checked, and that he is not aware of any material noncompliance with the order.[45] This is unlikely to be a significant counterweight to his more clearly defined fiduciary duty to shareholders, which duty all but requires him to maximize data collection.

The decision to impose documentation requirements, rather than bright line rules, represents a significant departure from how the government traditionally aims to protect the public. It is akin to if federal regulators, instead of ordering automakers to install seatbelts, ordered them to document the pros and cons of installing seatbelts, and to decide for themselves whether it would be worthwhile. This framework does not protect the public – it protects Facebook.[46]

B. The Proposed Privacy Committee of the Board of Directors is Largely Powerless

For repeat offender firms, regulators should consider seeking governance changes in addition to more traditional injunctive relief. This is because repeated lawbreaking is a sign that the governance structure has failed – either because leadership sanctioned profitable lawbreaking or because it failed to implement reasonable compliance controls.

Based on my observations, Facebook is a strong candidate for changes to its governance structure, a subject that is already of intense shareholder interest.[47] As detailed in the complaint, the company flagrantly broke the law even after it was ordered to stop – and that lawbreaking continued for years. Where was the company's board, and in particular its Audit Committee (now its Audit and Risk Oversight Committee), when these violations took place? Unfortunately, the proposed settlement ratifies Facebook's governance structure instead of changing it. The "Independent Privacy Committee" has little independence, no meaningful powers, and no buy-in from shareholders.[48] The Committee will be chosen by a nominating committee whose members

---

[45] Attestations by Facebook's CEO should not be interpreted as a means to hold him accountable for past violations. This relief is prospective only. In addition, some might compare these certifications to attestations under the Sarbanes-Oxley Act. 18 U.S.C. § 1350. Importantly, unlike the certifications required here, Sarbanes-Oxley Act certifications are tied to a measurable benchmark – accurate financial reporting pursuant to a known standard, e.g. GAAP.

[46] Settlement is the product of a compromise, and the majority is correct that litigation invites uncertainty about what a court would award. But our initial settlement demand should reflect the strongest relief we can obtain using all of our available tools, including our authority under 3.72(b) as well as civil penalty and equitable authorities. It should also be preceded by the company's full cooperation with a thorough investigation. I do not believe the proposed settlement reflects that approach.

[47] *See* SEC Proxy Statement filed by Facebook, Inc. (Apr. 12, 2019), http://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/ffdb441a-71d1-4bd0-9d7b-c1583143b218.pdf (reciting shareholder proposals to weaken Mark Zuckerberg's control of the company).

[48] Unlike other firms where control over the corporation is governed by "one-share, one-vote" principles, Facebook's existing governance structure provides "supervoting" rights for Class B shareholders. In this instance,

the controlling shareholder, Zuckerberg, can essentially pick or vote not to retain, reducing their level of independence. Even if truly independent directors were chosen, they would be virtually powerless: the order gives them no authority to veto any management decision, and their fiduciary duty is to shareholders, not users.[49]

Ultimately, the Committee's only clear power is to ensure that the company has assembled the paperwork required by the order. Corporate plans to integrate platforms, change terms of service, or other key decisions will be beyond the reach of the Committee, even if its members were sufficiently independent to want to intervene.

Given the ongoing concerns expressed by shareholders regarding Facebook's governance,[50] it is unwise for the FTC to accept a settlement that binds shareholders to a revised governance structure that may not further the goals of independence and accountability.

C. The Proposed $5 Billion Penalty May be Less than Facebook's Gains from Violating the Order

The Commissioners supporting the proposed settlement place great emphasis on the "record-breaking penalty." However, the Commissioners' analysis of the penalty is not empirically well grounded.

As noted above, when a company violates a Commission order, the agency can seek two distinct categories of monetary relief. First, the Commission can obtain equitable relief, including forfeiture of unjust gains (revenues and profits stemming from the violations) and refunds to consumers. This relief is not intended to be punitive; it is designed to reverse the effects of lawbreaking. Second, the Commission can seek civil penalties, which can be sought *in addition to* equitable relief. Civil penalties should send an unambiguous message that "FTC orders should not be disregarded with impunity."[51]

The Commissioners supporting the proposed penalty do not cite any methodology or analysis on Facebook's unjust enrichment from violating the Commission's order. In my view, a rigorous analysis of unjust enrichment alone – which, notably, the Commission can seek without the assistance of the Attorney General – would likely yield a figure well above $5 billion. As described earlier, Facebook's lawbreaking contributed directly to its drive for dominance and

---

the CEO, Mark Zuckerberg, controls more voting rights than his actual equity participation in the firm. He has such substantial rights that his vote is determinative with respect to the election of board directors and other matters subject to a shareholder vote.

[49] The proposed order requires the support of two-thirds of the voting power of outstanding shares to remove any committee member, but midterm removal of directors is highly unusual, and is unlikely to be necessary given the Committee's limited authority to restrain management. In any event, Mark Zuckerberg controls nearly 60% of the voting shares.

[50] *See, e.g.*, Michael Hiltzik, *Column: Facebook Shareholders are Getting Fed Up with Zuckerberg but Can't Do Anything about Him*, L.A. TIMES: BUSINESS (Apr. 16, 2019, 11:17 AM), https://www.latimes.com/business/hiltzik/la-fi-hiltzik-mark-zuckerberg-facebook-20190416-story.html.

[51] *U.S. v. Bos. Sci. Corp.*, 253 F. Supp. 2d 85, 101 (D. Mass. 2003) (awarding more than $7 million in civil penalties based on antitrust order violations).

profits, especially in the mobile space. The gains it realized from this lawbreaking were likely massive, especially given the large number of users who may have opted out of sharing had they known how. This would have significantly affected Facebook's value proposition to developers and shareholders.

But even if $5 billion were a reasonable estimate of Facebook's unjust gains, it would be inadequate as a civil penalty. A civil penalty should *exceed* unjust gains – otherwise we are allowing a defendant to break even or even profit by breaking the law. This approach is both common sense and grounded in Commission precedent: in the FTC's 2012 order enforcement against Google, we obtained a penalty that was more than five times the company's estimated unjust gains.[52]

Comparing the $5 billion figure in absolute terms to other FTC privacy settlements says little about this matter, in which Facebook is charged with an unprecedented assault on user privacy over many years.[53] My colleagues do not assert, as our predecessors did in *Google*, that the penalty proposed today exceeds Facebook's unjust gains five times over, which is a far more rigorous measure than absolute comparisons alone.

Were we to litigate, then, we would surely face risks – but so would Facebook. Eliminating unjust gains is only one of the five factors courts consider in imposing civil penalties: also considered are injury to the public, the defendant's ability to pay, the defendant's good or bad faith, and the necessity of vindicating the authority of the FTC.[54] In my view, each of these factors would support a penalty beyond the disgorgement of ill-gotten gains.

First, the harm to the public is substantial – Facebook's deceit affected tens of millions of Americans, and ultimately posed dangers to the democratic process.[55] Second, Facebook has vast assets, significant liquidity, and massive cash flows. Third, I do not believe the company has operated in good faith. Even while under order with the FTC, the company never came forward

---

[52] After the FTC's proposed settlement with Google was challenged in court as being inadequate, the Commission responded that "Google's penalty was many times over the upper-bound of what the FTC estimates the company earned from the alleged violation[.]" United States' Resp. to Consumer Watchdog's Amicus Curiae Br., *United States v. Google, Inc.*, No. 3:12-CV-04177-SI, 2012 WL 13080180, at *9–10 (N.D. Cal. Sept. 28, 2012) (comparing estimated unjust gains of $4 million to the $22.5 million civil penalty).

[53] The Commissioners supporting the settlement compare this penalty to what European Union regulators can obtain under the General Data Protection Regulation, but ignore that the Complaint filed today charges Facebook with numerous violations over numerous years, which under GDPR could have exposed the company to far greater fines, bans on information processing, and private claims for damages. *What if My Company/Organisation Fails to Comply with the Data Protection Rules?*, EUROPEAN COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en (last visited July 22, 2019).

[54] *See United States v. Reader's Digest Ass'n, Inc.*, 662 F.2d 955 (3d Cir. 1981) (setting out the standard considerations for civil penalties in cases involving order violations).

[55] The Commission's Complaint against Kogan – being filed concurrently with this action – details how political consultants exploited gaps in Facebook's privacy program to target millions of American users. It is likely that if Facebook had not used its privacy settings to trick users, many would have opted out of sharing their information with friends' third-party apps, which would have substantially diminished the impact of the election manipulation efforts.

to report its myriad violations, which persisted even after our investigation began.[56] Finally, Facebook's repeated abuses of user privacy while under order by the FTC undermined the public's confidence in our agency and in law enforcement generally. I do not believe a $5 billion penalty, especially as part of a settlement that otherwise blesses the company's business model, will restore the public's confidence or vindicate our authority.

There is one final reason to be concerned about our civil penalty analysis: In my view, we resolved this matter without finding out key facts about individuals' involvement in Facebook's lawbreaking. By settling, the Commission – and the public – may never find out what Facebook knows. Given what I believe is a clear information asymmetry, it is difficult to conclude that the Commission got the better end of the bargain.

D. The Settlement Immunizes the Firm for Undisclosed Violations

In agreeing to this proposed settlement, the majority has opted to give Facebook a legal shield of unusual, if not unprecedented, breadth, covering a wide range of conduct not addressed in the proposed complaint or settlement. This shield represents a major win for Facebook, but leaves the public in the dark as to how the company violated the law, and what violations if any are going unaddressed.

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 Commission is releasing both all known Section 5 claims *and* any and all order violation claims, whether known or unknown, concealed[57] or disclosed. Facebook also does not admit any wrongdoing, nor are there formal findings of fact about its misconduct.

The release of Section 5 violations is considerably broader than it may sound, and leaves major questions unanswered. Section 5 prohibits unfair or deceptive practices[58] – a vast category. Furthermore, many consumer protection statutes – such as the Children's Online Privacy Protection Act ("COPPA") – state that violations of their requirements constitute violations of the FTC Act.[59] This means that the proposed release not only shields Facebook from "known" (an undefined term) Section 5 claims, but also "known" claims under COPPA and other statutes. Given persistent questions about Facebook's compliance with these statutes,[60] the Commission should be transparent about which claims are being released – even if they are being released

---

[56] *See* Compl. ¶ 8 (charging that Facebook had private arrangements with developers until at least June 2018). Notably, "multiple violations over many years" can be an indicator of bad faith. *See U.S. v. Nat'l Fin. Servs., Inc.*, 98 F.3d 131, 140 (4th Cir. 1996) (affirming a penalty award based in part on repeated violations).

[57] If the Commission can later demonstrate that there was active concealment, it is possible a court would disregard the plain terms of the release. But the terms read how they read, and do not account for the good or bad faith of the Defendant in self-reporting violations.

[58] 15 U.S.C. § 45.

[59] 15 U.S.C. § 6505.

[60] *See, e.g.*, David Cohen, *Kids Groups are Urging the FTC to Investigate Facebook Over In-Game Purchases*, ADWEEK (Feb. 21, 2019), https://www.adweek.com/digital/kids-groups-are-urging-the-ftc-to-investigate-facebook-over-in-game-purchases/; *Child Advocates File FTC Complaint Against Facebook Kids' App*, VOANEWS.COM (Oct. 3, 2018, 12:24 PM), https://www.voanews.com/silicon-valley-technology/child-advocates-file-ftc-complaint-against-facebook-kids-app.

because they are seen as lacking viability. The public interest weighs strongly in favor of transparency, rather than secret immunity deals.

Also concerning is the Commission's proposed release of any and all order violations. As detailed above, the Commission's 2012 order barred Facebook from deceiving the public about its privacy policies, and required the company to create and maintain a reasonable privacy program subject to outside assessments. Over the course of this investigation, the Commission uncovered serious and repeated violations of this order. But even thorough investigations miss problems, and even well-counseled companies fail to disclose (or even conceal) violations. Allowing blanket immunity for unknown claims effectively rewards Facebook for not proactively disclosing its failures, even as the company is still not admitting those failures. This is a highly concerning message for a law enforcement agency to send.

Importantly, there were alternatives to a release of this breadth. While all settlements involve some release of claims, the Commission could have sought to expressly reserve certain categories of claims – a provision that the DOJ has obtained repeatedly, especially regarding claims against individuals.[61] Alternatively, the Commission could have shared with the public what "known" claims if any (e.g. those under COPPA) it was releasing, or required that Facebook attest that it was not aware of any additional violations.[62] These measures would have gone a long way toward giving the public more confidence in the outcome.

E. Facebook Obtained an Unusual Legal Shield for Mark Zuckerberg, Sheryl Sandberg, and Other Officers and Directors

Releasing claims against individuals can certainly be appropriate when their role has been thoroughly investigated, including through probing document review and examination under oath. But in this matter, the Commissioners supporting this settlement cannot cite any documents, sworn testimony, or other evidence to justify the broad immunity we are granting Mark Zuckerberg, Sheryl Sandberg, and others.

It is deeply problematic that we would award these individuals a blanket release and shield them from accountability. The insufficient scrutiny of these individuals deviates from FTC practice and Department of Justice guidelines. When it comes to small firms, Commission staff routinely investigates, deposes, and charges individual executives – including for privacy violations.[63]

---

[61] *See, e.g.*, Agreement for Compromise Settlement and Release, *United States v. Barclays Capital Inc., et al.*, No. 16-CV-7057 (KAM/JO) (E.D.N.Y. Apr. 24, 2018), ECF No. 137, at 6, https://www.justice.gov/opa/press-release/file/1047101/download (reserving claims against individuals other than the named Defendants); Proposed Final Judgment as to Defendant SK Energy Co., *United States v. Caltex Corp., et al.*, No. 18-CV-01456-ALM-CMV (S.D. Ohio Nov. 14, 2018), ECF No. 7-1, Att. 1 at 6, https://www.justice.gov/atr/case-document/file/1111316/download (reserving claims relating to "[a]ny liability of individuals[.]").

[62] In *Caltex,* for example, an action under the False Claims Act, the relator attested that it was not aware of any violations beyond what was alleged in the complaint. *Id.* at Att. 1, 4-5. The Commission or Facebook could have made a similar disclosure.

[63] Recent cases in which the Commission charged individuals with privacy violations include ClixSense, iDressup, and BLU Products. *See James V. Grago, Jr. also d/b/a ClixSense.com*, Matter No. 1723003 (June 19, 2019) (decision and order), https://www.ftc.gov/system/files/documents/cases/172_3003_clixsense_decision_and_order_7-2-19.pdf; *U.S. v. Unixiz, Inc. d/b/a i-Dressup.com et al.*, No. 5:19-CV-2222 (N.D. Cal. Apr. 24, 2019) (proposed stipulated order), https://www.ftc.gov/system/files/documents/cases/i-dressup_stipulated_order_ecf_4-24-19.pdf;

That is because the Commission rightly understands that when individuals make a calculated decision to break or ignore the law, they – and not just their firm or shareholders – should be held accountable.[64] To instead expressly shield individuals from accountability is dubious as a matter of policy and precedent.

The blanket release in today's proposed settlement also collides head-on with the DOJ's own guidelines for corporate investigations. In the aftermath of the financial crisis, where there was concern about the lack of individual accountability for Wall Street executives, the DOJ instituted guidelines requiring that individuals be investigated from the inception of a corporate investigation.[65] If DOJ attorneys opt to settle with the company before that investigation is completed, the guidelines instruct, they should ensure that the settlement preserves claims against individuals.[66] The Commission's proposed order does the opposite, releasing instead of reserving individual claims without citing any evidence to justify the decision.

The proposed grant of broad immunity is highly unusual. It is a departure from FTC precedent and established guidelines. Americans should ask why Mark Zuckerberg, Sheryl Sandberg, and other executives are being given this treatment, while leaders of small firms routinely face investigations, hearings, and charges. Law enforcement should enforce the law equally.

VI. Conclusion

In this matter, I believe that the Commissioners cut off the inquiry too early, leaving too many stones unturned, in favor of this proposed settlement. The fine print in this settlement gives Facebook a lot to celebrate, particularly when it comes to the blanket immunity for unspecified violations by Facebook and its executives. This is a disappointing precedent for the FTC to set, since more companies may now seek ways to buy broad immunity.

The press-driven price tag approach taken by enforcers is not only inappropriate – it is also unfair. Large incumbents can easily afford to bankroll the kind of blockbuster settlements that generate headlines. The small companies that can't pay away their legal problems face enforcers willing to wield their full authority and allocate substantial resources to hold them accountable.

We see this clearly in the FTC's disparate treatment of Facebook, where individuals are explicitly released, and Cambridge Analytica, where the former CEO was charged. This uneven approach to justice can lock in the market failures and imbalances that created the legal problems in the first place. It also reinforces a company's incumbency advantage both by allowing it to benefit from breaking the law and by holding smaller competitors to a different standard.

BLU Products, Inc. et al., Matter No. 1723025 (Sept. 6, 2018) (decision and order), https://www.ftc.gov/system/files/documents/cases/172_3025_c4657_blu_decision_and_order_9-10-18.pdf.

[64] It is important to note that the Commission does not *need* to obtain sworn testimony in order to charge an individual, and frequently does so based on other evidence. In my view, however, if we are going to grant an individual a broad release, that release should be based on compelling evidence, including sworn testimony, that demonstrates a lack of culpability.

[65] Policy Statement on Individual Liability, DEPT. OF JUSTICE, https://www.justice.gov/archives/dag/individual-accountability; later codified and revised as part of the Justice Manual at 4-3.100(1) (last updated Nov. 2018), https://www.justice.gov/jm/jm-4-3000-compromising-and-closing.

[66] *Id.* at 4-3.100(4).

We should have continued the investigation to obtain more data and evidence on what Facebook and its executives knew and how they profited. If Facebook failed to cooperate, the Commission had enough evidence to take Facebook and Zuckerberg to trial.[67]

When companies can violate the law, pay big penalties, and still turn a profit while keeping their business model intact, enforcement agencies cannot claim victory. If we cannot fix these problems, then policymakers must come together here at home and around the world to confront business models that rely on surveillance and profit from manipulation.

Nearly fifty years ago, Congress passed the Fair Credit Reporting Act to crack down on the business model of surreptitious collection and monetization of personal data. Since then, credit reporting companies have been legally required to adhere to a host of consumer protections such as providing free, periodic access to credit reports, correcting errors in the reports, and keeping people's information safe. Despite these protections, the credit reporting market remains a big pain point for consumers. That's because the law didn't fix the flawed financial incentives of a business model where consumers aren't the customer – they are the product. Our society and economy experience ongoing harm from these market distortions. Ubiquitous technology platforms built on the behavioral advertising business model raise similar concerns. This model will never be compatible with privacy unless we correct those incentives.

It is now more important than ever for global regulators and policymakers to address the threats posed by behavioral advertising. Absent an effective framework, we need to ask whether we need a moratorium on behavioral advertising by dominant platforms. We should question whether the traditional approach to privacy protection could ever fix these flaws. We need to determine whether immunities granted by decades-old laws are compatible with this business model. We need to make sure that the business model is not foreclosing competition and innovation.

Citizens and societies around the world are seeing how major technology platforms are not bringing us closer together in the way we thought they would. The behavioral advertising business model is broken, and we cannot let it continue to tear us apart.

[67] If Commissioners were concerned about litigation risk around our injunctive relief, we could have pursued a Commission proceeding under Rule 3.72(b) to modify the 2012 order to include bans and restrictions on data collection and changes to other business practices to address the fundamental incentive problems. A new final order would be subject to judicial review, but would be accorded substantial deference. I would have also supported a complaint for civil penalties under Section 5(l) of the FTC Act or a complaint for equitable monetary relief under Section 13(b) of the FTC Act if Facebook failed to cooperate with further investigation.