TECH FREEDOM

Honorable Charles "Chuck" Grassley
Chairman, Committee on the Judiciary
135 Hart Senate Office Building
Washington, D.C. 20510

Honorable Diane Feinstein
Ranking Member, Committee on the Judiciary
331 Hart Senate Office Building
Washington, D.C. 20510

Honorable John Thune
Chairman, Committee on Commerce, Science, and Transportation
511 Dirksen Senate Office Building
Washington, D.C. 20510

Honorable Bill Nelson
Ranking Member, Committee on Commerce, Science, and Transportation
716 Hart Senate Office Building
Washington, D.C. 20510

Honorable Greg Walden
Chairman, Committee on Energy and Commerce
2185 Rayburn House Office Building
Washington, D.C. 20515

Honorable Frank Pallone, Jr.
Ranking Member, Committee on Energy and Commerce
237 Cannon House Office Building
Washington, D.C. 20515

April 10, 2018

Re: April 10 Senate Hearing: "Facebook, Social Media Privacy and the Use and Abuse of Data" & April 11 House Hearing: "Facebook: Transparency and Use of Consumer Data"

Dear Chairmen Grassley, Thune, and Walden, and Ranking Members Feinstein, Nelson, and Pallone:

As your respective Committees prepare to question Facebook CEO Mark Zuckerberg regarding his company's handling of user data, we write to share our legal analysis of this important case, based on the public record. We also write to explain how consumer protection and other legal principles should guide both the Federal Trade Commission (FTC) in handling this matter and Congress in considering any new legislation.

Your Committees could play an important role in helping, through sworn testimony and responses to questions, to build a complete record of what happened in this case. But we urge

you not to rush into legislation. Haste makes for poor legislation, and indignation, however justified, is a poor basis for drafting the laws that will shape not only the future governance of Facebook, but that of every other Internet social network. Most critically, that includes the *next* "Facebooks." Whatever a revised regulatory framework might look like, today's entrenched incumbents can handle that regulatory burden far better than the startups vying to unseat them—especially since new companies, to attract users, must create radically innovative paradigms of user experience, while incumbents can far more easily afford to "play it safe."

While government has a vital role to play in protecting users, ultimately, the best protector of users is not government, but the possibility of disruption: no government sanction will ever do more to discipline Facebook than the possibility of its users leaving the site, or simply using it less, in favor of an alternative. This has been made very clear by the #DeleteFacebook campaign over the past month. Indeed, if the current public demand for Facebook accountability isn't enough, Facebook need only look to their predecessor—MySpace—to understand the unpredictability of online leadership, and how quickly incumbents can be dethroned by, perhaps, a more privacy-focused replacement.

The first response should come from the FTC, which is best able to explain the applicability of existing law to the facts of this situation. That analysis will be essential to Congress in identifying any shortcomings in existing law—which Congress should ask the FTC to do now.

We hold no brief for Facebook.[1] In fact, we believe that there *should* be a legal sanction in cases like this, but it is essential to distinguish among three distinct issues and, for each, three legal/policy questions. We summarize our conclusions below:

	Time Period	**Unfair or Deceptive Act?**	**Violation of 2011 Consent Decree?**	**Merits New Legislation?**
Allowing app developers to access data of users' friends	Through April 2014 (until FB policy change)	No	No	No
Failure to notify users of misuse	December 2015 (*Guardian* story) - present	**Potential deception by material omission**	No	**Yes**: part of larger breach notification law
Failure to stop misuse once notified	Early 2016 - present	No	No	**Maybe** if tied to specific trigger (*e.g.*, election interference)

[1] Facebook has been one of many supporters of TechFreedom's work. We have never received project-specific support from Facebook, nor do we take direction in our work from Facebook or any other donor.

The attached appendix explains our conclusions in greater detail. Here, we summarize six key principles underlying all consumer protection law—both current and potential—and how such considerations should guide Congress and the FTC in handling this matter:

1. **Customer Notification:** The FTC Act's prohibition of "deception" has always been the FTC's primary tool for policing new technologies, and there would be nothing inappropriate or unusual about the FTC relying solely on deception in this case. Indeed, we believe the FTC should be able to bring a deception charge against Facebook given Facebook's failure to notify its users of GSR's violation of its policies in transferring data to Cambridge Analytica. This omission was likely "material"—the key requirement of the FTC's Deception Policy Statement[2]—given the unique sensitivity of concerns about Russian interference in the 2016 U.S. election. Facebook's decision *not* to notify users about Cambridge Analytica's misuse of data about them (until now) denied Facebook users the opportunity to decide whether to avoid such use of their data— most obviously, by quitting Facebook. Still, the FTC has little experience defining materiality in any analytically rigorous way; for this and other reasons, the FTC is not well-positioned to decide, across the board, when customer notification is and is not required. For years, Congress has been considering potential federal legislation governing when companies are required to be notified when information is accessed without authorization.[3] We would, in principle, support such legislation. Congress should start by asking the FTC to take public comment on the issue before issuing a report to Congress explaining the varying degrees of sensitivity and complex relationships involved, as well as recommending an appropriate statutory framework to govern them. At a minimum, a company in Facebook's situation should be required to notify the Federal Election Commission (FEC), if not its users.
2. **Election Interference:** Understanding that the FTC will likely be able to hold Facebook accountable for failing to notify its users, coupled with the fact that the FTC is, in fact, currently conducting its own investigation to gather more information, we urge Congress to approach new legislation cautiously. Doing so will allow Congress

[2] The Deception Policy Statement asks "whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception." FED. TRADE COMM'N, FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc*., 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[3] Cambridge Analytica's acquisition of information from GSR, the app developer, did not constitute a "security breach," but nonetheless constituted the acquisition of data in excess of authorization of the terms of service under which GSR originally collected the data. Some state notification laws would likely have applied here.

to focus its efforts on how to craft a response to the overriding issue here—foreign interference with elections and the manipulation of voters more generally—in ways that are consistent with the First Amendment and minimize unintended consequences for the Internet ecosystem.

3. **The First Amendment:** The Supreme Court has only begun grappling with how to reconcile concerns about the misuse of data with the First Amendment. But the Court's first major decision in this area, *Sorrell v. IMS Health*, strongly suggests that the Court will, as it almost always does, err on the side of protecting free speech interests. The *Sorrell* court overturned a state law requiring that doctors opt-in before information collected about the kinds of prescriptions they write could be used to target drug advertising to them. Writing for the majority, Justice Kennedy wrote, "Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes."[4]
4. **Unfairness & Duty of Care:** The FTC may consider charging Facebook with unfair business practices for failing to do more than it did to prevent further misuse of user data by Cambridge Analytica—most notably, by requiring an audit rather than relying on a certification by the company that it had ceased using Facebook user data acquired from GSR in violation of Facebook's terms of service. We are sympathetic to such arguments and believe that there may be a way to legislate a narrowly tailored duty to guard against misuse in circumstances like this one, where Facebook received clear notice, via *The Guardian*, that Cambridge Analytica was misusing Facebook data on behalf of foreign parties to influence the 2016 election. But imposing such liability via unfairness could have sweeping, unintended consequences for the entire Internet ecosystem: holding *every* data collector responsible for preventing *any* misuse by the third-party companies to whom it transfers data or, even more remotely, by the fourth-party companies to which those third-parties might transfer data (even when barred from doing so by their agreements with the data collector) is the kind of broad liability that has been limited to statutorily defined common carriers.[5] Such a standard would be even more improper in cases like this, where, under the terms of the 2011 Consent Order, the FTC itself reviewed, and seemingly blessed, Facebook's policies. Congress *has* created specific, statutory liability

[4] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011).

[5] *See, e.g.*, 47 U.S.C. § 222.

schemes, and could do so here, but if it does, it should focus on clear, definable problems, such as knowledge might be misusing data in an attempt to influence the U.S. election.

5. **Third-Party Sharing:** Some may attempt to suggest that Facebook's pre-April-2014 policy of allowing an application developer to access information about the friends of the users of their app was inherently problematic, and that all such data access should require opt-in. This would mark a radical departure from the FTC's longstanding approach, which requires opt-in only for sensitive, non-public information.[6] In general, requiring more opt-ins harms users by encouraging developers to seek opt-ins with excessive scope, and de-sensitizing users to privacy choices that really matter.[7] It would also tend to benefit large app developers over small ones, and platforms like Facebook over their developers.[8] Users benefit from apps that make data available about their friends—such as by notifying them in their desktop or mobile calendar about their friends' birthdays. They also benefit from the fact that such services are available outside of Facebook. Legally restricting the third party sharing of information would simply help to perpetuate and extend Facebook's dominance over what users do online.
6. **Caution about Broadly Construing Consent Orders:** We urge caution in trying to expand the scope of consent orders, such as Facebook's 2011 agreement with the FTC, to cover conduct that was not clearly "fenced in" by the original decree. Unlike Section 5, whose unfairness and deception standards were framed in deliberately broad terms, consent decrees should be interpreted narrowly, like any contract, to give effect to what *both* parties understood the agreement to be at the time. Subsequently reinterpreting the terms of a negotiated settlement to cover conduct they did not believe it would cover raises serious due process concerns about fairness to the regulated party. It would also violate well-established principles of tort liability, which bar holding one party responsible when an intervening party is the "superseding cause" of harm to another. Finally, it would end up harming consumers: broad construction of consent decrees may have the perverse result of discouraging companies like Facebook from reporting, or investigating, misuse.

---

[6] FED. TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter *2012 Privacy Report*].

[7] Nicklas Lundblad & Betsy Masiello, Opt-in Dystopias, 7 SCRIPTed 155, 162-64 (2010), https://script-ed.org/wp-content/uploads/2016/07/7-1-Lundblad.pdf.

[8] *Id*. at 164.

We are highly skeptical that any attempt to craft broad, "comprehensive privacy" legislation will produce a bill that will do more good than harm to the Internet ecosystem. But careful consideration of these principles should help lawmakers to draft simple, manageable, and flexible pieces of legislation targeted at real problems—starting with the lack of notification to users and law enforcement agencies, including both the FTC and FEC.

We stand ready to assist your Committees as you consider legislation, and how to task the FTC with the right questions to be answered before Congress legislates.

Respectfully,

Berin Szóka
President
TechFreedom

Graham Owens
Legal Fellow
TechFreedom

Appendix

I. Consumer Protection Law, both Existing and Potential

Available information suggests that the FTC would be successful in arguing that Facebook made a material omission that would constitute deception under Section 5 of the FTC Act. More generally, we believe that companies like Facebook should have a legal duty to more carefully scrutinize the use of data by how their third-party partners, and the fourth parties to whom they may, in turn, transfer data. However, we are skeptical that a failure to adequately police such misuse, such as by requiring audits, could be based on the FTC's unfairness authority, which requires a clearer showing of injury, and may not be grounded primarily in public policy considerations.

We would, nevertheless, support legislation to address the kind of public policy consideration at issue here: foreign interference with elections and the manipulation of voters more generally. Finally, based on the evidence available to us, we doubt that Facebook's conduct violated its 2011 consent decree and urge caution in trying to expand the scope of such consent decrees to cover conduct that was not clearly "fenced in" by the original decree. Subsequently reinterpreting the terms of a negotiated settlement to cover conduct the regulated party did not expect it to cover would cover raises serious due process concerns. Reinterpreting a consent decree may also end up harming consumers: broad construction of consent decrees may have the perverse result of discouraging companies like Facebook from reporting, or investigating, misuse. We suspect this may have happened here, that Facebook may have been less willing to report the misuse of user data by Cambridge Analytica, and to audit the company to ensure such use ceased, because it was subject to a consent decree.

A. Deception: Material Omission in Failing to Notify Users

It appears that Facebook first became aware that Cambridge Analytica was using data harvested about Facebook users—in violation of Facebook's terms of service—to create "psychographic profiles" that allowed the targeting of ads in support of the Republican primary

campaign of Sen. Ted Cruz (R-TX), thanks to a December 2015 report in *The Guardian*.[9] Yet Facebook failed to notify its users of this violation of its own policies.

This failure may have constituted a deceptive practice under Section 5 of the FTC Act, which applies to omissions as well as affirmative misstatements—provided they are "material." Materiality is the focus of the FTC's 1983 Deception Policy Statement, which asks "whether the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. If so, the practice is material, and consumer injury is likely, because consumers are likely to have chosen differently but for the deception."[10] In this case, "choosing differently" may mean not only leaving the site altogether, but also using it less, or taking advantage of Facebook's privacy controls to restrict the availability of user data. Facebook's failure, over more than two years, to inform its users of the misuse of their information—and thus the potential for similar misuse by other companies—denied consumers the ability to make such choices.

It is not exactly clear how the FTC would assess the materiality of this information, since the FTC has brought relatively few material omission cases and, in its affirmative misstatement cases (in privacy and data security), has generally skipped this step, instead relying on a provision of the 1983 Deception Policy Statement that allows the FTC to presume that any explicit statement is presumptively material.[11] Nonetheless, we do not believe it would be difficult for the agency to establish materiality here. The fact that news of this misuse had become, to some degree, "public" with *The Guardian*'s publication in December 2015 does not excuse Facebook's failure to notify its users any more than a news report about a data security breach would excuse a company from its obligation to notify its customers about the breach (the failure to do so in a timely manner could constitute a material omission for the same reasons explained here, even absent state data breach notification laws). Most Facebook users did not learn of the *Guardian* story, and even those that did may not have understood its full implications. In either event, many Facebook users would still have made different choices if they had full information about how their data could be misused. The intense reaction of Facebook's users to this scandal over the last few weeks strongly suggests that news of this misuse of Facebook data would have been material to many Facebook users.

---

[9] Harry Davies, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*, THE GUARDIAN (Dec. 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[10] FED. TRADE COMM'N, FTC Policy Statement on Deception, *appended to Cliffdale Assocs., Inc*., 103 F.T.C. 110, 174 (1984), *available at* https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

[11] *Cf.* Geoffrey A. Manne, R. Ben Sperry & Berin Szoka, *In the Matter of Nomi Technologies, Inc.: The Dark Side of the FTC's Latest Feel-Good Case*, ICLE Antitrust & Consumer Protection Research Program White Paper 2015-1 (2015), http://laweconcenter.org/images/articles/icle-nomi_white_paper.pdf.

And it is important to remember that the period over which the failure to notify users extended from late 2015 through March 2018. Thus, it *is* fair to assess the materiality of this information to Facebook users both *after* the 2016 election and in light the crescendo of news in 2017 and early 2018 about Russian interference with the election via Facebook.

The FTC should have little difficulty bringing a deception charge against Facebook. The FTC Act's prohibition of deceptive acts and practices has always been the FTC's primary tool for policing new technologies, and there would be nothing inappropriate or unusual about the FTC relying solely on its deception power in this case.

B. Unfairness: Failure to Effectively Stop Misuse of User Data by Apps

It appears that Facebook responded promptly to the *Guardian* story by contacting Cambridge Analytica, SCL Elections, and Global Science Research to ask all three companies what data they had and to delete such data. Yet, even still, it is difficult to understand why the ensuing investigative process within these companies took so long, and why Facebook was willing to accept a certification from GSR in March of 2017 that it had deleted the relevant data—based solely on an internal audit—rather than requiring its own audit.

Failure to adequately verify deletion of the data *could* constitute an unfair trade practice, just as the FTC has charged dozens of companies with unfair trade practices for failing to adequately secure user data from breach by intruders.[12] It depends on the degree to which the injury suffered by Facebook users here is the kind of "substantial injury" Congress intended the FTC to police under Section 5(n) of the FTC act. The FTC's data security cases have generally involved financial data, whose revelation could cause significant, quantifiable injury to consumers.[13] Or, in some limited cases, the FTC has brought data security cases against companies which failed to secure highly sensitive information, such as about the use of antidepressants.[14] By contrast, the data at issue here is *not* financial; instead, the information

---

[12] *See, e.g.,* Press Release, Fed. Trade Comm'n, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017), https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data; Press Release, Fed. Trade Comm'n, *Operators of AshleyMadison.com Settle FTC, State Charges Resulting From 2015 Data Breach that Exposed 36 Million Users' Profile Information* (Dec. 14, 2016), https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting.

[13] *See, e.g.,* Press Release, Fed. Trade Comm'n, *BJ's Wholesale Club Settles FTC Charges: Agency Says Lax Security Compromised Thousands of Credit and Debit Cards* (June 16, 2015), https://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

[14] Press Release, Fed. Trade Comm'n, *Eli Lilly Settles FTC Charges Concerning Security Breach: Company Disclosed E-mail Addresses of 669 Subscribers to its Prozac Reminder Service* (Jan. 18, 2002), https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

gathered by GSR consisted of the "likes" of users and those of their friends. Taken in totality, these "likes" revealed enough about the user's personality that GSR and Cambridge Analytica were able to build "psychographic profiles" about users that could be used to target political ads to them. This raises very serious public policy concerns about the potential for foreign actors to manipulate American voters through Facebook, but that public policy consideration alone will not be enough to justify the FTC deeming Facebook's failure to require an audit to be an "unfair" trade practice.

In general, an unfair practice is one that (i) causes substantial injury to consumers that is (ii) not outweighed by any offsetting consumer or competitive benefits and that (iii) consumers could not reasonably have avoided.[15]

1. **Substantial injury:** At least some Facebook users clearly suffered *some* kind of injury from the continued misuse of their data beyond the point when an audit could have prevented that use.
2. **Countervailing benefit:** Of course, audits have costs, and those costs are ultimately borne by Facebook's users—if not in financial terms (since Facebook is a free service), then in the trade-offs Facebook must ultimately make: resources spent auditing companies suspected of misusing Facebook data are ultimately resources *not* spent on improving the site, policing user content, responding to other user complaints, *etc*.
3. **Avoidability by users:** Given Facebook's failure to notify its users of the breach, there is no way users could have reasonably prevented the injury at issue themselves.

The FTC's 2012 Privacy Report could be read to suggest that the particular Commissioners who voted to issue that report might have found a substantial injury in this case:

> The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the ***unexpected revelation of previously private information***, including both sensitive information (e.g., health information, precise geolocation information) and less sensitive information (e.g., purchase history, employment history) to unauthorized third parties. As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz. The creation of that social network in some cases

[15] *See* FED. TRADE COMM'N, FTC Policy Statement on Unfairness, *appended to Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), *available at* https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness;), available at https://www.ftc.gov/publicstatements/1980/12/ftc-policy-statement-unfairness [hereinafter 1980 Unfairness Policy Statement].

> revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful. Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[16]

While the Privacy Report did not specifically discuss the issue here—the potential responsibility to audit third party apps to prevent their use of data beyond what had been permitted—the failure to conduct an audit could well, under this approach, be considered a means by which the "unexpected revelation of previously private information … to unauthorized third parties" could occur.[17]

But there is good reason for skepticism about so expansive a view of injury—and therefore of the Commission's power over unfair trade practices. While the paragraph quoted above purports to be nothing more than a restatement of the FTC's past enforcement actions, it actually pushes both of the precedents cited far beyond what the Commission actually did in those cases. The first case is more directly comparable to the present Facebook case: In attempting to prepopulate its new social network, Google Buzz, Google had effectively revealed some "Gmail users' most frequent email contacts." That information was likely even more sensitive than the "likes" at issue here, yet the FTC brought only a deception case, which did not require proving "substantial injury." Nonetheless, in the 2012 Privacy Report, the FTC insisted, in a footnote, that it *could* have brought an unfairness case:

> Although the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. See Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), available at http://www.ftc.gov/opa/2011/03/google.shtm (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).[18]

This approach to unfairness might or might not be justified; it would depend on the particular facts of the case. But the fact that the Commission chose not to make such a claim in the

[16] 2012 Privacy Report, *supra* note 6, at 8.

[17] *Id*. at 8.

[18] *Id*. at 8, n. 37.

Buzz case indicates just how difficult it would be for the agency to convince a judge to accept such a theory of harm—and thus suggests reasons for hesitating to take such an approach here.

Likewise, the Report overstates the precedent set by the FTC's 2011 settlement with Facebook: "Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful."[19] Here is what the 2011 complaint against Facebook actually said:

> by designating certain user profile information publicly available that previously had been subject to privacy settings, Facebook materially changed its promises that users could keep such information private. ***Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent***, in a manner that has caused or has been likely to cause substantial injury to consumers, was not outweighed by countervailing benefits to consumers or to competition, and was not reasonably avoidable by consumers. This practice constitutes an unfair act or practice.[20]

It makes sense to presume consumers are being harmed when a company retroactively changes its privacy policy without getting their opt-in: such a bait-and-switch closely resembles deception, which is, after all, simply a species of unfairness where we can presume that users are harmed by not getting the benefit of material promises. (In fact, it may make more sense to bring such claims as deception cases.)

But that is not what happened in this case. Rather, the question is whether Facebook should have done more than it did to prevent further misuse of user data—again, such as by requiring audits. At a minimum, the 2012 Privacy Report does not answer this question.

Some "like" information may, in fact, be so sensitive that its use could constitute substantial injury, depending on how it was used. For example, in *Eli Lilly*, the pharmaceutical maker inadvertently shared the email addresses of more than 600 Prozac users, thus exposing them to reputational harm because of the sensitivity (at that time) of depression.[21] In *TrendNet,* a

---

[19] *Id*.

[20] Complaint at 29, In the Matter of Facebook, Inc., FTC File No. 092 3184, No. C-4365 (F.T.C. Nov. 29, 2011) [hereinafter Facebook Complaint], *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf (emphasis added).

[21] Press Release, Fed. Trade Comm'n, *Eli Lilly Settles FTC Charges Concerning Security Breach: Company Disclosed E-mail Addresses of 669 Subscribers to its Prozac Reminder Service* (Jan. 18, 2002), https://www.ftc.gov/news-events/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach.

the maker of web cameras had failed to correct a vulnerability that allowed anyone with the IP address to watch the video feed of a camera, thus potentially exposing the most intimate aspects of private conduct in the home to digital voyeurs.[22] Both examples seem significantly more sensitive than what we currently know of the information made available to Cambridge Analytica in this case. In an event, these are highly fact-dependent inquiry best left to the Commission.

In fact, the actual harm underlying the outrage in this case seems to be not about injury to any particular user, or even to all Facebook users collectively, but rather to our democracy overall. This is a legitimate and substantial public policy consideration that deserves law-makers' attention. But that does not mean it should be shoehorned into the unfairness standard. In the 1970s, following the Supreme Court's decision in *FTC v. Sperry & Hutchinson Co.,* , the FTC treated "violation of public policy" as an independent basis for a finding of unfairness.[23] This led to such an abuse of the FTC's sweeping powers to determine which trade practices are "unfair" that the FTC was dubbed the "National Nanny" by *The Washington Post*,[24] and the FTC, under Democratic leadership and under intense pressure from a Democratic Congress, narrowed its conception of unfairness to limit the use of public policy considerations in the 1980 Unfairness Policy Statement.[25] In 1994, Congress enacted Section 5(n), which provides that, "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[26]

This does not mean that public policy considerations are not a legitimate basis for government action; merely that Congress, rather than the FTC, should be responsible for deciding

---

[22] Complaint at 8, In the Matter of TrendNet, Inc., FTC File No. 122 3090, No. C-4426 (F.T.C. Jan. 16, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[23] 405 U.S. 233 (1972).

[24] Editorial, *The FTC as National Nanny*, WASHINGTON POST (March 1, 1978), https://www.washingtonpost.com/archive/politics/1978/03/01/the-ftc-as-national-nanny/69f778f5-8407-4df0-b0e9-7f1f8e826b3b/?utm_term=.db1c16c55d05; *see also* TechFreedom, *Thanks, FTC, But We Don't Need a National Nanny* (July 24, 2014), http://techfreedom.org/thanks-ftc-but-we-dont-need-a-national-nanny/.

[25] *See generally* J. Howard Beales, Former Director, Bureau of Consumer Protection, Fed. Trade, Comm'n, *The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection* (May 30, 2003), https://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-resurrection (outlining "the important role the FTC's unfairness authority can and should play in fashioning consumer protection policy," as well as "the rise, fall, and resurrection of unfairness - focusing on the lessons that the Commission has learned from its early experiences" where "the Commission's unfairness powers have been both used and avoided inappropriately.").

[26] 15 U.S.C. § 45(n).

how to address them. Congress has repeatedly given the FTC more specific statutory authority to deal with specific areas of concern, such as children's privacy and credit reporting. We would support legislation to clarify the FTC's authority in this situation—as discussed below.

C. Sharing of Data with Third Party App Developers

In April 2014, apparently shortly after Dr. Aleksandr Kogan, a lecturer at Cambridge University, had collected the "like" information of 87 million Facebook users who were friends with the 300,000 users of his "thisisyourdigitallife" app (offered by his company, Global Science Research), Facebook moved to sharply limit what information third party app developers could access through the site's API. First, Facebook announced that developers would not be able to access the Facebook friends list of a Facebook user who used their app without receiving the permission of those friends.[27] A week later, Facebook announced that "checkins, likes, photos, posts, videos, Events, and Groups, will require prior approval by Facebook" (but not necessarily users) and also that the API would no longer share potentially sensitive information, including, most notably, "religion and political views."[28]

In his testimony for this hearing, Zuckerberg summarizes these changes as follows:

> In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the Facebook information apps could access. Most importantly, apps like Kogan's could no longer ask for information about a person's friends unless their friends had also authorized the app. We also required developers to get approval from Facebook before they could request any data beyond a user's public profile, friend list, and email address. These actions would prevent any app like Kogan's from being able to access as much Facebook data today.[29]

Some may argue that Facebook's policy prior through early 2014 was itself a violation of Section 5. While this does not appear to be the focus of complaints against Facebook, we mention this here for the sake completeness. We are not currently aware of any allegation

---

[27] Ime Archibong, *Facebook Platform Changes in Development*, FACEBOOK DEVELOPERS NEWS BLOG (March 26, 2018), https://developers.facebook.com/blog/post/2018/03/26/facebook-platform-changes/.

[28] Other information that would not be shared with third-parties included "relationship status, relationship details, custom friend lists, about me, education history, work history, my website URL, book reading activity, fitness activity, music listening activity, video watch activity, news reading activity, games activity." Ime Archibong, *API and Other Platform Product Changes*, FACEBOOK DEVELOPERS NEWS BLOG (April 4, 2018), https://developers.facebook.com/blog/post/2018/04/04/facebook-api-platform-product-changes/.

[29] *Facebook: Transparency and Use of Consumer Data: Hearing Before the H. Comm. on Energy & Commerce* 115th Cong. 2 (2018) (statement of Mark Zuckerberg, Chairman & CEO, Facebook), http://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf.

that Facebook misled users about the availability to application developers of information about the friends of the users of their application—other than the general refrain that Facebook's privacy controls should be simple, in general. This would be a difficult charge to bring on unfairness grounds—and properly so. The argument that Facebook's policy was inherently unfair would be even more difficult to sustain, given the difficult trade-offs involved, especially from the perspective of Facebook at the time. Facebook has been criticized for years as being too "closed" a platform. Their 2014 change of policy arguably made the platform more "restrictive" and thus harder for app developers to compete with Facebook itself for features that Facebook might chose to build into the site. Privacy advocates would surely agree that Facebook made the right decision, but there were other values at stake that the Commission would have to weigh in any unfairness case.

D. Potential Violation of Facebook's 2011 Consent Order

In addition to charging Facebook with new violations of Section 5, the FTC might argue that Facebook's conduct in this matter violated the terms of the company's 2011 Consent Order with the FTC. We are highly skeptical of such claims as a legal matter and believe that construing settlements so broadly would have a host of unintended practical consequences.

Indeed, the Consent Order may have deterred Facebook from taking common sense measures—like notifying their customers and requiring an audit of Cambridge Analytica's use of information—that could have mitigated the problems currently before them. This would not be entirely surprising. Like prescriptive regulations, consent decrees often set "regulatory floors," encouraging companies to focus narrowly on what is specifically *required* of them in order to be compliant with the dictates of their regulator—which may mean doing *less* than the company would do if it were subject to a more general standard, such as Section 5 or the negligence standard of tort law. Process is never a substitute for judgment, yet such perverse incentives continue to be a byproduct of the FTC's arbitrary practice of regulation-by-settlement, which, as TechFreedom has noted in the past, "undermines the rule of law and harms consumers by deterring privacy disclosures."[30]

1. Background on the Consent Order

The 2011 Consent Order settled an FTC complaint that Facebook had "deceived consumers by telling them they could keep their information on Facebook private, and then repeatedly

[30] Press Release, TechFreedom, *FTC's Google Settlement a Pyrrhic Victory for Privacy and the Rule of Law* (Aug. 9, 2012), http://techfreedom.org/ftcs-google-settlement-a-pyrrhic-victory-for/.

allowing it to be shared and made public."[31] According to its complaint, "Facebook ha[d] represented, expressly or by implication, that, through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends."[32] However, according to the FTC, "[i]n truth and in fact, in many instances, users could not restrict access to their profile information to specific groups, such as 'Only Friends' or 'Friends of Friends' through their Profile Privacy Settings. Instead, such information could be accessed by Platform Applications that their Friends used."[33] Thus, according to the Commission, these misrepresentations constituted a "false or misleading representation" in violation of Section 5.[34]

Following the FTC's complaint, on November 29, 2011, the FTC announced a negotiated Consent Order settling the charges[35]—as the Commission has done with essentially every company charged with unreasonable data privacy practices before and since.[36] Facebook agreed, among other requirements, that it would not misrepresent the extent to which it maintains the privacy or security of certain user information, including the extent to which Facebook makes covered information available to third parties; that "prior to any sharing of a user's *nonpublic* information," Facebook will "obtain the user's affirmative express consent;" and that Facebook would establish, implement, and maintain a comprehensive privacy program designed to address privacy risks related to the development and management of new and existing products and services for consumers.[37]

Like all consent orders, the final Consent Order, issued on July 27, 2012, "admit[s] no liability" on the part of Facebook, focuses only "on prospective requirements on the defendant," and, as one court put it, is "of little use to [the defendant] in trying to understand the specific

---

[31] Press Release, Fed. Trade Comm'n, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises* (Nov. 29, 2011) [hereinafter FTC Facebook Press Release], available at https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-itdeceived-consumers-failing-keep.

[32] Complaint at 17-18, In the Matter of Facebook, Inc., FTC File No. 092 3184, No. C-4365 (F.T.C. Nov. 29, 2011), available at https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf.

[33] *Id*.

[34] *Id*. at 18.

[35] *See* FTC Facebook Press Release, *supra* note 31.

[36] Justin (Gus) Hurwitz, *Data Security and the FTC's Uncommon Law,* 101 Iowa L. Rev. 955, 972 (2016) ("To date the FTC has brought more than 50 data security actions; all but two of these actions have settled.").

[37] In the Matter of Facebook Inc., FTC File No. 092 3184, No. C-4365, at 3-6 (F.T.C. July 27, 2012) (consent order) [hereinafter Facebook Consent Order], available at https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf.

requirements imposed by [Section 5]."[38] This is because such orders are essentially settlement agreements that a judge agrees to enforce as a judgment, and thus, "bear some of the earmarks of judgments entered after litigations," but also "closely resemble contracts."[39]

2. Consent Orders Should Be Interpreted Narrowly, Like Any Contract.

Consent orders, or "decrees," are effectively contracts between the parties to litigation, which the judge agrees to enforce as a judgment.[40] As courts recognize, "that consent decrees involve an additional layer of 'judicial action' does not mean that we must ignore the many ways in which they resemble settlements."[41] Like any contract, they should be interpreted narrowly to give effect to what *both* parties understood them to mean. Indeed, where a consent decree goes beyond the terms originally agreed to by the parties to affect third parties or effectively promulgates an amendment or change to a statute—such as the unfairness standard under Section 5—without following proper procedures, courts have invalidated them as an improper rulemaking. In *Conservation Northwest v. Sherman*, the Ninth Circuit recognized this in holding a consent decree improper:

> It follows that where a consent decree *does* promulgate a new substantive rule, or where the changes wrought by the decree are *permanent* rather than temporary, the decree may run afoul of statutory rulemaking procedures even though it is in form a "judicial act." We therefore hold that a district court abuses its discretion when it enters a consent decree that permanently and substantially amends an agency rule that would have otherwise been subject to statutory rulemaking procedures.[42]

Unlike Section 5, whose unfairness and deception standards were framed in deliberately broad terms through proper congressional statutory procedures, consent decrees should be interpreted narrowly, as any contract would be, to only give effect to the terms agreed to by the parties'. They should also be interpreted narrowly to avoid affecting the rights of parties outside the suit, who were afforded no opportunity to comment or in any way participate in deciding the decree's terms, or otherwise have consequences beyond the dispute between the original parties. Subsequently reinterpreting the terms of a negotiated settlement to

---

[38] *FTC. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 257 n.22 (3d Cir. 2015).

[39] *Local No. 93, Int'l Ass'n of Firefighters v. City of Cleveland*, 478 U.S. 501, 519 (1986).

[40] *See United States v. State of Or.*, 913 F.2d 576, 580 (9th Cir. 1990) ("A consent decree is 'essentially a settlement agreement subject to continued judicial policing.'") (quoting *Williams v. Vukovich*, 720 F.2d 909, 920 (6th Cir. 1983)); *see also* Larry Kramer, *Consent Decrees and the Rights of Third Parties*, 87 Mich. L. Rev. 321, 325 (1988).

[41] *Conservation Northwest v. Sherman*, 715 F.3d 1181, 1188 (9th Cir. 2013) (citing *Local 93*, 478 U.S. at 519).

[42] *Id.* at 1187.

cover conduct they did not believe it would cover raises serious due process concerns about fairness to the regulated party. It would also violate well-established principles of tort liability, which bar holding one party responsible when an intervening party is the "superseding cause" of harm to another. Finally, it would end up harming consumers: broad construction of consent decrees may have the perverse result of discouraging companies like Facebook from reporting, or investigating, misuse.

3. General Principles of Tort Law Bar Holding Facebook Liable when an "Intervening Party" is the "Superseding Cause" of Harm.

Finding that Facebook violated its consent decree by failing to prevent misuse of data by Cambridge Analytica would violate well-established principles of tort law that allow a negligent party to be held responsible for harm caused by an intervening third party only in narrow circumstances. The Restatement of Torts provides that:

> A superseding cause is an act of a third person or other force which by its intervention prevents the actor from being liable for harm to another which his antecedent negligence is a substantial factor in bringing about.[43]

Facebook appears to satisfy *all* of the factors set forth by the Restatement. We provide our analysis following each provision of the Restatement

> *The following considerations are of importance in determining whether an intervening force is a superseding cause of harm to another:*
>
> *(a) the fact that its intervention brings about harm different in kind from that which would otherwise have resulted from the actor's negligence;*[44]

The data at issue, what pages users like, is benign on its own. Only when used to create psychographic profiles could it result in the kind of harm alleged here.

> *(b) the fact that its operation or the consequences thereof appear after the event to be extraordinary rather than normal in view of the circumstances existing at the time of its operation;*

There is no way Facebook could have predicted that Cambridge Analytica's misuse of Facebook user information could sway the results of the 2016 election.

---

[43] Restatement (Second) of Torts § 440 (Am. Law Inst. 1965) *available at* https://www.scribd.com/document/112246702/Restate-2d-superseding-cause-excerpts [hereinafter *Restatement*].

[44] *Id*. § 442.

> *(c) the fact that the intervening force is operating independently of any situation created by the actor's negligence, or, on the other hand, is or is not a normal result of such a situation;*

It is difficult to see how Facebook could have been negligent in allowing GSR to collect data in the first place—unless one argues that *all* sharing of friend data to third party app developers was negligent *per se*. Rather, Facebook's negligence occurred later, once it had been notified that the misuse had occurred.

> *(d) the fact that the operation of the intervening force is due to a third person's act or to his failure to act;*

Cambridge Analytica appears to have acted entirely independent of Facebook.

> *(e) the fact that the intervening force is due to an act of a third person which is wrongful toward the other and as such subjects the third person to liability to him;*
>
> *(f) the degree of culpability of a wrongful act of a third person which sets the intervening force in motion.*

Cambridge Analytica violated Facebook's terms of service and then falsely certified to Facebook that it had deleted that data.

In short, in this case, Cambridge Analytica appears to qualify for *all* the factors required to be a "superseding cause" of harm for which Facebook cannot reasonably be held liable.

4. Detailed Analysis of Facebook's Compliance with Each of the Consent Order's Requirements

The 2011 Consent Order required Facebook to comply with nine specific restrictions, all of which are in effect for 20 years.[45] If Facebook violates any one of these requirements, it is liable for a civil penalty of $41,484 for *each* violation of the Order.[46] To illustrate why we do not believe, based on currently available information, Facebook violated the Order, we discuss the first six provisions of the Order, as well as the ninth provision's reporting requirement, which appear most relevant.

Order I: First, the Order states that Facebook, "in connection with any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication,

[45] Facebook Consent Order, *supra* note 37, at 8 ("This order will terminate on July 27, 2032, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint … in federal court alleging any violation of the order, whichever comes later.").

[46] 16 C.F.R. § 1.98(c).

the extent to which it maintains the privacy or security of covered information," including, "the extent to which Respondent makes or has made covered information accessible to third parties."[47] This raises two distinct legal issues.

First, even if Facebook's failure to properly notify its users of the specific instance of Cambridge Analytica's misuse of the data *does* constitute a material omission actionable under Section 5, it likely does *not* constitute a "misrepresentation" under the Order for the simple reason that the Consent Order clearly refers to Facebook's own practices and its interaction with third parties; Facebook's interactions with fourth parties would be beyond the scope of the consent decree. Further, if the FTC believed Facebook's policies to be inadequate, they had multiple opportunities to say so. Under the terms of the Order, Facebook was required to "establish, implement, and maintain an comprehensive privacy program,"[48] "implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party from servers under Respondent's control after a reasonable period of time,"[49] and "obtain initial and biennial assessments and reports from a qualified … third-party,"[50] all of which had to be submitted to the FTC for review.[51]

Second, and more generally, Facebook cannot be accused of failing to notify its users that their information might become public. Facebook's data policy at the time made clear what constitutes public and nonpublic information, including explicitly warning users that "[a]s a general rule, you should assume that if you do not see a sharing icon, the information will be publicly available."[52] Further, the policy clearly warns users that their information may be accessible to the developers of apps used by their friends unless they opt-out of Facebook apps completely:

> If you want to completely block applications from getting your information when your friends and others use them, you will need to turn off all Platform applications. This means that you will no longer be able to use any third-party Facebook-integrated games, applications or websites.

---

[47] Facebook Consent Order, *supra* note 37, at 3.

[48] *Id*. at 5.

[49] *Id*. at 5.

[50] *Id*. at 6.

[51] *Id*. at 8.

[52] Facebook, 2013 Data Use Policy (Date of Last Revision: Nov. 15, 2013), *available at* https://web.archive.org/web/20140521181947/https://www.facebook.com/full_data_use_policy. For the sake of simplicity, we chose to analyze the 2013 Facebook Data Use Policy, which appears to have been in place when most Facebook users would have participated in the GSR app in question.

> If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.[53]

This policy, regardless of whether Facebook's users took the time to read it, provides clear notice that their data could be used by third parties and is likely "publicly available." As such, it is difficult to see what "misrepresentation" Facebook could have committed about its privacy practices in general. Further, as Facebook explains, "Aleksandr Kogan requested and gained access to information from users who chose to sign up to his app, and everyone involved gave their consent."[54] As those using the third-party app "knowingly provided their information," it is unlikely that the FTC could argue that Facebook misrepresented that this event would occur, and even took steps beyond mere notice by acquiring consent from users of the app. Note that Dr. Kogan (through his company, GSR) lied to Facebook and violated its privacy policies by passing the data to Cambridge Analytica. If anyone misrepresented "the extent to which it maintains the privacy or security of covered information" it was Dr. Kogan (or GSR), not Facebook.

Order II: The Order mandated that Facebook,

> prior to any sharing of a user's nonpublic user information … with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall:
> (A) clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document:
> (1) the categories of nonpublic user information that will be disclosed to such third parties,
> (2) the identity or specific categories of such third parties, and
> (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and
> (B) obtain the user's affirmative express consent.[55]

---

[53] *Id*.

[54] Paul Grewal, VP & Deputy General Counsel, Facebook, *Suspending Cambridge Analytica and SCL Group from Facebook,* FACEBOOK NEWS ROOM (March 16, 2018), https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

[55] Facebook Consent Order, *supra* note 37, at 4.

Yet the Order also expressly states that "[n]othing in Part II will … require [Facebook] to obtain affirmative express consent for sharing of a user's nonpublic information initiated by another user authorized to access such information."[56]

Facebook could not have violated this provision of the Order because it (1) obtained consent from all users of the GSR app, and (2) informed users that the data shared (*e.g.*, "likes," comments, check-ins, etc.) was public user information, not the "nonpublic user information" covered by the Order. Further, although no clear consent was obtained from by users that participated in the GSR app to share with Cambridge Analytica, it was the researcher, an authorized third-party user, that initiated the unauthorized transfer of data. Facebook, upon discovering that the data was being misused, requested that the data be destroyed, and subsequently received confirmation that they had been destroyed.

Order III: The Order required Facebook, "no later than sixty (60) days after the date of service of this order," to "implement procedures reasonably designed to ensure that covered information cannot be accessed by any third party *from servers under Respondent's control*…."[57] As the information that was improperly shared came from Dr. Kogan and not "servers under [Facebook's] control, there can be no violation of this provision, regardless of the "reasonableness" of Facebook's policies.

Order IV and IX: Facebook was required to "establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."[58] The Order further stated that, "[s]uch program, the content and implementation of which must be documented in writing, shall contain controls and procedures appropriate to [Facebook's] size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the covered information, including … the development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information."[59]

---

[56] *Id*.

[57] *Id*. at 5.

[58] Facebook Consent Order, *supra* note 37, at 5.

[59] *Id.* (emphasis added).

In addition to developing and implementing this program, the Order also required that Facebook, "within ninety days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth the manner and form of their compliance with this order."[60] Thus, because the FTC had sufficient opportunities to review and accept/decline Facebook's proposed policy program, a finding that the program was somehow ineffective retroactively would not only be unfair to Facebook, which was itself a victim of a third party's "superseding" intervention.

Data security and privacy both pose a unique challenge: unlike other unfairness cases, the company at issue is both the victim (of data breaches) and the culprit (for allegedly having inadequate data security). In such circumstances, the FTC's approach should be grounded in tort principles of negligence, rather than strict liability. Even as the country's chief regulator and expert on data security, the FTC was unable to specify the practices that would prevent all future losses of data—illustrating just how difficult such cases can be.

Order VI: The Order required Facebook to "maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of" information related to the company's privacy policies and compliance with the Order, including: "(A) … all widely disseminated statements by Respondent or its representatives that describe the extent to which Respondent maintains and protects the privacy, security, and confidentiality of any covered information;" "(B) … all consumer complaints directed at Respondent or forwarded to Respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;" and "any documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent's compliance with this order."[61]

It was recently revealed that Facebook had "deleted some messages sent by Zuckerberg to other Facebook users via Messenger or Facebook's chat tools going back as far as 2010." [62] It is possible that this could have violated the FTC's 2011 consent decree, which required Facebook to "maintain and upon request make available to the Federal Trade Commission" certain information regarding the company and its privacy practices, should it be determined

[60] *Id*. at 8.

[61] Facebook Consent Order, *supra* note 37, at 7.

[62] Michael Grothaus, *Facebook deleted messages sent by Mark Zuckerberg from recipients' inboxes*, Fast Company (April 6, 2018), https://www.fastcompany.com/40555344/facebook-deleted-messages-sent-by-mark-zuckerberg-from-recipients-inboxes.

that the deleted messages contained information covered by the Order and were therefore improperly deleted.

However, in a statement to *TechCrunch,* Facebook claimed that the move was "done for corporate security" and Facebook "did so in full compliance with our legal obligations to preserve messages."[63] Given that under judicially entered consent decrees, if either party fails to fulfill their obligations under the agreement, the other party can ask the court to find the party in contempt without having to file a new lawsuit for breach of contract, it seems unlikely that Facebook would risk a $40,000 per violation (*e.g.*, per deleted message pertaining to the Order), and risk contempt over Facebook messages.[64] Thus, while that is for the FTC to determine and we encourage the FTC to enforce the specific requirements of the Order, agreed to by Facebook to settle the FTC's 2011 investigation, the current facts available do not indicate a violation of the Consent Decree.

5. Broad Concerns with Consent Orders as Highlighted by Facebook's Case

Courts and federal agencies have both played critical roles in the development of law in the United States. English judges began developing today's common law long before the colonization of America.[65] Since the creation of the Interstate Commerce Commission in 1887,[66] federal agencies have developed regulations governing a broad range of industries and areas, including everything from the environment[67] to the Internet.[68] These two institutions of American law, in conjunction with the Legislative Branch, have generally worked together in harmony, with agencies promulgating rules and regulations derived from Congressional grants of power, and enforcing them through litigation in the courts.

As a general rule, in order for any agency to create legally binding norms through rules and regulations, it must follow certain statutorily required procedures—generally, those set

---

[63] Josh Constine, *Facebook retracted Zuckerberg's messages from recipients' inboxes*, TechCrunch (April 6, 2018), https://techcrunch.com/2018/04/05/zuckerberg-deleted-messages/.

[64] Susan B. Dorfman, *Mandatory Consent: Binding Unrepresented Third Parties Through Consent Decrees*, 78 MARQ. L. REV. 153, 155 (1994).

[65] See Victor E. Schwartz et al., Prosser, Wade & Schwartz's Torts: Cases and Materials 1 (12th ed. 2010) ("[T]ort law has been principally a part of the common law, developed by the courts through the opinions of the judges in the cases before them.").

[66] *See generally* Richard A. Epstein, Why the Modern Administrative State Is Inconsistent with the Rule of Law, 3 NYU J.L. & Liberty 491 (2008).

[67] See Massachusetts v. EPA, 549 U.S. 497, 532 (2007) (stating that the Clean Air Act authorizes federal regulation of emissions of carbon dioxide by the Environmental Protection Agency).

[68] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (2017) (restricting the online collection of personal information from children under the age of 13).

forth in the Administrative Procedure Act ("APA").[69] These procedural rules ensure that any party which may be adversely affected by a proposed regulation has adequate notice of the potentially forthcoming regulation, as well as the opportunity to comment on its prudence and impact before it takes effect.[70] Further, while the APA sets the minimum degree of public participation an agency must provide, "[matters] of great importance, or those where the public submission of facts will be either useful to the agency or a protection to the public, should naturally be accorded more elaborate public procedures."[71]

Despite this procedural framework and the historically harmonious relationship between the three coequal federal branches of government, a trend has formed over the past two decades where federal agencies—particularly the FTC—have begun to more frequently utilize consent decrees,[72] "as a technique to shape agencies' regulatory agendas, without input from the public or the regulated community."[73] By avoiding public input, federal agencies have essentially started utilizing consent decree settlements as a means of circumventing the traditional regulatory development and review process.[74]

Consent decrees are supposed to remedy the harm in the specific cases to which they are derived—not to make it easier for the FTC to bring enforcement actions against the company for subsequent conduct that is materially different from the conduct that led to the consent decrees. Yet the FTC has exhibited a troubling tendency to use consent decrees to impose its policy preferences, usually as stated in nominally non-binding reports (following workshops organized by the Commission itself and generally designed to produce the outcome desired by Commission staff); to bypass the requirements of unfairness and deception, as set forth in the FTC's policy statements and Section 5(n); and to impose monetary penalties.

The most notable example is the FTC's 2012 order—imposing a $22.5 million fine, the largest ever for violation of an FTC consent decree—against Google for allegedly violating its 2011

---

[69] *See* Administrative Procedure Act, 5 U.S.C. §§ 500-596 (2012).

[70] *Id*. § 553 (2012); *see also Nat'l Petroleum Refiners Ass'n v. F.T.C*., 482 F.2d 672, 692 (D.C. Cir. 1973) ("[U]nder the Administrative Procedure Act the public, including all parties in the industry who might be affected, are given a significant opportunity prior to promulgation of a rule to ventilate the policy and empirical issues at stake through written submissions, at a minimum.").

[71] Administrative Procedure Act: Legislative History, S. Doc. No. 248, at 259 (1946).

[72] *See* Sue and Settle: Regulating Behind Closed Doors, U.S. Chamber of Commerce (2013), https://www.uschamber.com/sites/default/files/documents/files/SUEANDSETTLEREPORT-Final.pdf.

[73] H.R. Rep. No. 114-184, at 4 (2015).

[74] *Id.*

consent decree regarding the Buzz social network.[75] The FTC alleged that Google had deceived users of Apple's Safari browser by failing to update a single online help page that provided instructions regarding how to configure a privacy setting applicable to Google tracking tools inside Safari after *Apple* changed how the browser worked. This conduct bore no relationship to the 2011 *Buzz* settlement, which, as described above, involved attempting to prepopulate its new social network in ways that exposed some users' potentially sensitive most-emailed contacts.[76] Most critically, in understanding why this constituted an abuse of the consent decree process, the FTC failed to conduct any analysis of the materiality—which is the lodestar of the Deception Policy Statement—of Google's statements; indeed, the order does not even mention materiality once. This may indicate that the FTC believes it is not required to establish the requirements of Section 5 when alleging the violation of the consent decree, because a pure misstatement, *regardless of materiality*, will suffice as a violation.

Interpreting consent decrees in so broad a manner raises several concerns. Most general is that the FTC is effectively using the decrees to turn Section 5 into the basis for regulating the entire Internet ecosystem—with stiff penalties. It's akin to being put on probation after agreeing to a suspended sentence for a speeding ticket and then, for the next twenty years (the length of essentially *all* FTC consent decrees) being subject to immediate arrest and heavy fine for even minor infractions, without the protection of the usual requirements of proof. More specifically, FTC consent decrees, unlike antitrust consent decrees, are not subject to judicial approval, and thus lack the safeguard that review by an independent, neutral tribunal provides. Second, such consent decrees may not be in the public interest. As former Commissioner Thomas Rosch argued in 2011,

> There should be internal and procedural safeguards to ensure that consent decrees do indeed serve the public interest when they are being accepted or approved by an agency. With respect to the Commission, the public interest is critical because it is what cabins the "wide discretion" that we otherwise wield to fashion remedial orders that only have to bear a "reasonable relation to the unlawful practices found to exist.[77]

---

[75] Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[76] *See supra* note 11.

[77] J. THOMAS ROSCH, FORMER COMMISSIONER, FED. TRADE COMM'N, REMARKS BEFORE THE XVIIITH ST. GALLEN INTERNATIONAL COMPETITION LAW FORUM AT THE UNIVERSITÄT ST. GALLEN ST. GALLEN, SWITZERLAND 2 (April 7, 2011), https://www.ftc.gov/sites/default/files/documents/public_statements/consent-decrees-public-getting-its-moneys-worth/110407roschconsentdecrees.pdf.

Finally, the FTC does allow for public comment on its consent decrees, but there is little reason to think the Commission actually listens: the agency has "never withdrawn a proposed consent decree based on comments we have received," as Commissioner Rosch noted in 2011.[78]

If anything, Congress should be studying how to prevent the FTC from expanding its consent decrees beyond their original scope. The last thing Congress should do is encourage such behavior.

II. Potential Legislation

We believe this case raises significant public policy concerns, particularly regarding foreign interference in American elections. Existing consumer protection law may address some of those concerns, but it would be a mistake to expect the Federal Trade Commission to address all these concerns through its current legal authority.

Yet another kind of mistake would be to enact overly broad, prescriptive legislation. Instead, Congress should, in addition to letting the FTC pursue the consumer protection aspects of this case through its existing authority, focus its attention on carefully targeting legislation to those issues that the FTC may not be legally able to, or be in the best position to, address. Even the thing most likely to be actionable under the FTC Act today—the lack of user notification from Facebook—would be far better addressed through legislation than by expecting the FTC to police when such notifications should be required more generally under its Unfairness power.

A. Privacy & Breach Notification Legislation

Congress has been debating what is commonly called "baseline comprehensive privacy legislation" for eighteen years.[79] We are highly skeptical that the legislative process will produce a broad bill that will do more good than harm to the Internet ecosystem. Europe's approach to this issue, the soon-to-become-effective General Data Protection Regulation (GDPR) demonstrates the pitfalls of attempting to legislate a single, all-encompassing "solution" to privacy concerns. Instead, we encourage lawmakers to focus on three relatively simple, manageable pieces of legislation.

---

[78] *Id*.

[79] *See, e.g.,* MICROSOFT, BASELINE PRIVACY LEGISLATION (Feb. 2013); Cameron F. Kerry, *States Lead Washington on Consumer Privacy Laws*, BROOKINGS INSTITUTE (Aug. 3, 2016), https://www.brookings.edu/blog/techtank/2016/08/03/states-lead-washington-on-consumer-privacy-laws/ (noting Former President Obama's proposed Consumer Privacy Bill of Rights, "which establishes a set of baseline consumer and business expectations").

We have long supported a federal standard for breach notification. This would replace the existing patchwork of state bills regarding breach notification with a single, nationwide standard. As is appropriate for clear, specific regulations (unlike the FTC's broad, general authority under Section 5), the FTC should be able to impose civil penalties for violations of such rules.

If this incident has changed anything, it is that it illustrates why it may be appropriate to expand the scope of such notification requirements from data security breaches to scenarios like this one, where a third party has obtained data not through a technical security breach but because Party B (the third party app developer) collected the information from Party A (a social network), then transferred that data to Party C (a fourth party such as Cambridge Analytica) in violation of the terms of service by which Party B obtained the information from Party A. While we believe that Party A's failure to notify its users of the misuse of information by Parties B and C may constitute deception, including such situations in a data breach notification law may help ensure timely notification of consumers.

Mandating such notifications is the simplest, cleanest form of government intervention, and should be preferred over any attempt to dictate what sites can and cannot do with user data. It would also ensure that regulators are fully informed. The best way to proceed with such legislation would be to ask the FTC and FEC for recommendations.

B. Duty to Investigate/Audit

Requiring websites to audit *every* third-party app's use of data, and even every "suspicious app's" use of data, is not only impractical (especially for sites smaller than Facebook); it would also likely prove counter-productive, by distracting limited resources from the most suspicious apps. Imposing such broad liability could significantly disrupt the Internet ecosystem. The burden of such liability would fall hardest not on Facebook but on its smaller competitors. Again, under basic American tort law, even negligent parties cannot be held liable for harm that results from the superseding cause of another's intervention except in narrow circumstances.[80]

In limited circumstances, it could be appropriate for Congress to craft legislation that hold data collectors like Facebook responsible, for preventing the misuse of data collected through their site by third parties—including the transfer of that information (in violation of the terms of service under which it was initially collected by the third party) to fourth parties, who subsequently misuse it. But these circumstances must be narrowly tailored to real harms and clearly defined. For example, where a company has been credibly notified—such

[80] *See supra* at 17.

as Facebook was by *The Guardian*'s 2015 story—that its data is being misused to influence an American election, and especially where that influence may involve a foreign party, it may be appropriate for that company to have a special duty of care, which could require that the company take additional measures to prevent misuse, such as by requiring an audit to ensure that the data is no longer being used.

The best way to proceed with such legislation would be to ask the FTC and FEC for recommendations.

Even without a legal mandate to do so, Facebook seems—if belatedly—to be taking the approach that its critics want. As Zuckerberg explains:

> We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected.

C. FTC Process Reform Legislation

We encourage Congress to perform a more systemic reassessment of the FTC's current practices and procedures—especially in the context of enforcement actions and settlements. We believe that carefully tailored process reforms could make the FTC's operations more transparent, and thus make the FTC more effective in guiding companies to take reasonable measures to protect consumers.

Rather than repeat the full analysis white paper we presented to the House Energy & Commerce Committee in 2016,[81] and to the Senate Commerce Committee last fall,[82] we have instead provided a short overview of how to consider thinking about the main process reforms we believe need to be addressed through legislation.

1. **More Economic Analysis:** As many commentators have noted, the FTC has frequently failed to employ sufficient economic analysis in both its enforcement work and policymaking. Former Commissioner Josh Wright summarized the problem

[81] *See* BERIN SZÓKA & GEOFFREY A. MANNE, THE FEDERAL TRADE COMMISSION: RESTORING CONGRESSIONAL OVERSIGHT OF THE SECOND NATIONAL LEGISLATURE 57-60 (2016), *available at* http://docs.house.gov/meetings/IF/IF17/20160524/104976/HHRG-114-IF17-Wstate-ManneG-20160524-SD004.pdf [hereinafter White Paper].

[82] *FTC Stakeholder Perspectives: Reform Proposals to Improve Fairness, Innovation, and Consumer Welfare Hearing Before the Subcomm. on Consumer Protection, Product Safety, Insurance, and Data Security of the S. Comm. on Commerce, Science, & Transp.* 115th Cong. (2017) (statement of Berin Szoka, President, & Graham Owens, Legal Fellow, TechFreedom), http://docs.techfreedom.org/Szoka_FTC_Reform_Testimony_9-26-17.pdf.

pointedly in a speech entitled "The FTC and Privacy Regulation: The Missing Role of Economics," explaining:

> An economic approach to privacy regulation is guided by the tradeoff between the consumer welfare benefits of these new and enhanced products and services against the potential harm to consumers, both of which arise from the same free flow and exchange of data. Unfortunately, government regulators have instead been slow, and at times outright reluctant, to embrace the flow of data. What I saw during my time at the FTC is what appears to be a generalized apprehension about the collection and use of data – whether or not the data is actually personally identifiable or sensitive – along with a corresponding, and arguably crippling, fear about the possible misuse of such data.[83]

As Wright further noted, such an approach would take into account the risk of abuses that will cause consumer harm, weighed with as much precision as possible. Failing to do so can lead to significant problems, including creating disincentives for companies to innovate and create benefits for consumers. Specifically, Congress or the FTC should require the Bureau of Economics to have a role in commenting on consent decrees[84] and proposed rulemaking,[85] and a greater role in the CID process. But the most effective ways to engage economists in the FTC's decision-making would be to raise the FTC's pleading standards and make reforms to the CID process designed to make litigation more likely: in both cases, the FTC will have to engage its economists more closely, either in order to ensure that its complaints are well-plead or to prevail on the merits in federal court.

2. **Clarification of the FTC's Substantive Standards:** The FTC has departed in significant ways from both the letter and spirit of the 1980 Unfairness Policy Statement and the 1983 Deception Policy Statement. This is mainly due to the FTC essentially having complete, unchecked, discretion to interpret these policy statements as it sees fit — including the discretion to change course regularly without notice. The courts simply have not had the opportunity to effectively implement Section 5(n), nor has the FTC ever really chosen to constrain its own discretion in meaningful ways (as it has done with the Green Guides). Making substantive clarifications to Section 5 will not be adequate without *process* reforms to ensure that these clarifications are given effect over time. But that does not mean they would be without value. In order to clarify the

---

[83] Remarks of Joshua D. Wright, *The FTC and Privacy Regulation: The Missing Role of Economics*, George Mason University Law and Economics Center (Nov. 12, 2015), *available at* http://masonlec.org/site/rte_uploads/files/Wright_PRIVACYSPEECH_FINALv2_PRINT.pdf.

[84] *See* White Paper, *supra* note **Error! Bookmark not defined.**, at 42-43.

[85] *See id*. at 98-100.

FTC's substantive standards under Section 5, we would suggest the following key changes:

1. Codifying other key aspects of the 1980 Unfairness Policy Statement into Section 5 that were not already added by the addition of Section 5(n) in 1994;
2. Codifying the Deception Policy Statement, just as Congress codified the Unfairness Policy Statement in a new Section 5(n).[86] Specifically, in codifying the Deception Policy Statement, Congress should require the FTC to meet the requirements of Section 5(n) when bringing enforcement actions based on the "reasonableness" of a company's practices, such as data security.[87]
3. Codify the FTC's 2015 Unfair Methods of Competition Policy Statement, with one small modification: the FTC should be barred from going beyond antitrust doctrine.[88]

3. **Clarifying the FTC's Pleading Standards:** Several courts have already concluded that the FTC's deception enforcement actions must satisfy the heightened pleading standards of Section 9(b) of the Federal Rules of Civil Procedure, which applies to claims filed in federal court that "sound in fraud."[89] As explained below, this requirement would not be difficult for the FTC to meet, since the agency has broad Civil Investigative powers that are not available to normal plaintiffs before filing a complaint.[90] There is no reason the FTC should not have to plead its deception claims with specificity. The same can be said for unfairness claims, even though they do not "sound in fraud." In both cases, getting the FTC to file more particularized complaints is critical, given that the FTC's complaint is, in essentially all cases, the FTC's last word on the matter, supplemented by little more than a press release, and an aid for public comment.
4. **Encouraging More Litigation to Engage the Courts in the Development of Section 5 Doctrine and Provide More Authoritative Guidance:** Litigation is important for two reasons. First, having to prove its case before a neutral tribunal forces analytical rigor upon the FTC and thus forces it to make better, more informed decisions.

---

[86] *See* White Paper, *supra* note **Error! Bookmark not defined.**, at 21-28.

[87] *See infra* 89.

[88] *See* White Paper, *supra* note **Error! Bookmark not defined.**, at 28-30; Fed. Trade Comm'n, Statement of Enforcement Principles Regarding "Unfair Methods of Competition" Under Section 5 of the FTC Act (Aug. 13, 2015), available at https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf.

[89] Rombach v. Chang, 355 F.3d 164, 170 (2d Cir. 2004) ("In deciding this issue, several circuits have distinguished between allegations of fraud and allegations of negligence, applying Rule 9(b) only to claims pleaded under Section 11 and Section 12(a)(2) that sound in fraud.").

[90] *See infra* at 19.

Second, court decisions will provide guidance to regulated companies on how to comply with the law that is necessarily more authoritative (since the FTC cannot simply overrule a court decision the way it can change its mind about its own enforcement actions or guidance) and also likely (but not necessarily) more detailed and better grounded in the FTC's doctrines. One major reason companies settle so often across the board is that the FTC staff has the discretion to force companies to endure the process of litigating through the FTC's own administrative process, first before an administrative law judge and then before the Commission itself, before ever having the opportunity to go before an independent, neutral tribunal. We generally suggest the following three options:[91]

1. "[E]mpower one or two Commissioners to insist that the Commission bring a particular complaint in Federal court. This would allow them to steer cases out of Part III either because they are doctrinally significant or because the Commissioners fear that, unless the case goes to federal court, the defendant will simply settle, thus denying the entire legal system the benefits of litigation in building the FTC's doctrines. In particular, it would be a way for Commissioners to act on the dissenting recommendations of staff, particularly the Bureau of Economics, about cases that are problematic from either a legal or policy perspective."[92]
2. Abolish Part III completely, as former Commissioner Calvani has proposed.[93]
3. Require the FTC to litigate in federal court while potentially still preserving Part III for the supervision of the settlement process and discovery.[94] Requiring the FTC to litigate all cases in federal court (as the SMARTER Act would do for competition cases[95]) might, in principle, prove problematic for the Bureau of Consumer Protection, which handles many smaller cases. Retaining Part III but allowing Commissioners to object to its use might strike the best balance.

D. The Honest Ads Act

Much of the media attention surrounding this incident has focused on the Honest Ads Act as a solution.[96] However, nothing in that bill would have prevented the harm at issue in this case: the misuse of information about what users are interested in to create psychographic

[91] *See* White Paper, *supra* note **Error! Bookmark not defined.**, at 82-85.

[92] *Id.*

[93] *See id*. at 84-85.

[94] *Id.*

[95] Standard Merger and Acquisition Reviews Through Equal Rules Act of 2015, H.R. 2745, 114th Cong. (2015).

[96] Honest Ads Act, S. 1989, 115th Cong. (2017).

profiles that could be used to influence their views of the election. As explained above, we *do* believe Congress could craft narrowly tailored legislation to address that problem, but it would look nothing like the Honest Ads Act. The bill focuses solely on the purchase of advertising (not an issue here) by foreign persons, imposing a duty on social media sites like Facebook to scrutinize the eligibility of parties that *might* be foreign persons to buy political ads. We have serious practical and constitutional concerns about this bill, which we would be happy to explain to your Committee staff.