Fox in the Henhouse: The Delegation of Regulatory and Privacy Enforcement to Big Tech

William Bendix
Dakota State University
William.Bendix@dsu.edu

Jon MacKay
The University of Auckland
jon.mackay@auckland.ac.nz

Abstract

The Federal Trade Commission (FTC) has ordered tech giants to police the app developers that use their platforms, requiring them to remove apps that employ deceitful sales tactics or violate consumer privacy. Tech giants have often resisted FTC orders to police the companies on their platforms because policing takes significant resources and diminishes profits. But some firms, after paying modest fines for neglecting enforcement, have eventually complied with FTC demands, removing predatory apps and banning problematic developers. Other firms have continued to shirk enforcement obligations at the risk of escalating fines. What accounts for the differences? Using process tracing to track decisions by Apple and Facebook, we find that tech giants willingly police consumer fraud but not consumer privacy violations. Failures to police fraud leads to public complaints and negative press attention, while failures to police data breaches often go undetected by consumers, the media, and thus the FTC.

1. Introduction

Overburdened as watchdogs, some federal agencies recruit industry-leading companies to conduct regulatory oversight on the US government's behalf. Such companies, known as "enforcer firms," are legally required to monitor the many business partners they work alongside and to make sure these partners operate in full compliance with the law [1]. If they shirk or ignore the oversight responsibilities imposed on them, enforcer firms can face serious penalties themselves—even if they have committed no legal violations otherwise. In the case of the high-tech sector, the Federal Trade Commission (FTC) has ordered tech giants to police the app developers that use their platforms and social networks, requiring them to remove apps that employ deceitful sales tactics or violate consumer privacy. Big tech enforcers have tended to resist FTC orders because enforcement activities cut into their revenues [1], [2]. But some firms, after paying modest fines for neglecting oversight, have eventually complied with FTC demands, flagging predatory apps and permanently blocking problematic developers. Other tech giants, however, have repeatedly shirked enforcement requirements at the risk of escalating sanctions.

What accounts for the differences in performance? To answer this question, we explore the principal-agent relationship between the FTC and two tech giants—Apple and Facebook—tracking each company's response to regulatory orders across a ten-year period, from 2010 to 2020. Initially, both firms decided to ignore the agency's enforcement requests and let app developers commit ongoing legal and privacy violations. Apple allowed developers to trick children into making unauthorized in-app purchases on their parents' accounts. Facebook, meanwhile, gave developers broad access to its users' personal data, even after assuring users their information was protected. Eventually Apple complied with FTC orders in full, while Facebook committed ongoing policing failures.

These differences among the companies are puzzling because both have similar advantages over the FTC and can easily commit to a non-enforcement strategy. With the technical capacity to conceal or misrepresent violations and with immense financial resources to absorb large fines, they can assume the risks of ignoring government regulators [3]. To explain differences in firm behavior, we use process-tracing methods to develop detailed case studies on Apple and Facebook, examining the terms of their enforcement requirements, documenting their interactions with the FTC, tracking their policing efforts over time, and identifying any intervening factors that help account for enforcer compliance and defiance. Public documents from both the government and the companies provide the necessary materials to assemble these case studies.

In the end, we find that the nature of violations by app developers was the decisive factor in determining whether tech giants willingly conducted enforcement. When parents learned that their children had made unauthorized in-app purchases from billing statements, many of them complained to Apple about the charges. Their complaints gained the news media's interest and the FTC's attention, and soon after the policing failures of both firms were exposed. Moreover, Apple could reasonably anticipate that consumer complaints would

URI: https://hdl.handle.net/10125/79653
978-0-9981331-5-7

only increase, and that FTC investigations would inevitably follow, if they continued to ignore the sales strategies of app developers. But when it came to fraudulent data-harvesting practices, there were no customer complaints or opportunity for such complaints to trigger investigations. Because data from Facebook were secretly retrieved, both the public and the FTC could not know the extent of the privacy violations or the level of neglect by the tech enforcer. Furthermore, Facebook could reasonably calculate that disclosure of its data practices was unlikely and that FTC orders were largely toothless. Our analysis thus offers one clear lesson: that without a predictable alarm mechanism, such as public complaints and press scrutiny, tech giants are unlikely to restrain their business partners, uphold privacy interests, and comply with federal requirements to enforce regulations.

1.1 Recruiting Enforcer Firms

We are accustomed to viewing the relations between government regulators and private firms as inherently antagonistic—and for good reason. The fields of law, economics, and political science have produced enormous evidence showing that similar conflicts play out across many different industries [4]–[6] While federal agencies seek the best strategies for corporate enforcement, many firms seek the best strategies for noncompliance, regulatory capture, or both. But some companies, despite these adversarial conditions, are required to help federal agencies conduct regulatory tasks. These companies have been dubbed "enforcer firms" [1].

An enforcer firm is a large, industry-leading company that has been instructed by the US government to monitor and police some of the third parties it hires or does business with. On one level, the process of recruiting enforcer firms is rather straightforward. Congress simply passes legislation that grants oversight authority to a federal agency and the agency in turn delegates some of its authority to a major company. But there is some complexity to the delegation process, especially if a company resists or neglects its enforcement role. To start, an agency must find a statutory basis for compelling companies to monitor the commercial practices of their business partners. Once it has done so, the agency informs the companies of their new responsibilities and then investigates them periodically to make sure they are monitoring the third parties under their purview. If the agency finds serious or blatant lapses in enforcement, it can levy fines against a firm for delinquency and issue a legal order compelling the company to follow specific policing instructions. Major companies across industries—including banking, oil, and high tech—carry out enforcement tasks for the federal government [1], [7].

Enforcers in each industry operate under the scrutiny of different regulatory agencies. For the high-tech sector, the Federal Trade Commission serves as the main government watchdog. The FTC, as an independent regulatory commission, has the authority to investigate any commercial activities that are potentially "unfair or deceptive" (Federal Trade Commission Act). It also has the authority to investigate activities that potentially undermine consumer privacy, including online privacy [8], [9]. Under these two broad mandates, the FTC has required the largest tech companies—including Apple and Facebook—to monitor third parties that use or sell products through the online platforms and networks these companies operate. The FTC has issued two types of orders along these lines. First, it has ordered tech giants to monitor their platforms for any predatory or fraudulent practices used by third-party developers to sell apps or other online products. Second, the FTC has ordered tech giants to protect the digital privacy of their users, even after having shared user data with third parties. This second order requires tech giants to audit third parties and determine whether they are maintaining the privacy and security of user data [1], [2].

As noted above, leading firms in other industries face similar legal requirements to monitor third parties, but their enforcement roles differ somewhat from those of the tech giants. Firms in other industries are mostly responsible for third-party surrogates that carry out services on their behalf. Credit card companies that hire independent call centers must make sure that these centers do not mislead customers about credit card fees and options. Similarly, oil companies that hire excavation firms must make sure that these contractors maintain safety and environmental standards on drill sites [1]. For tech giants, rather than monitoring surrogates, they police the use of their own networks, platforms, and data by other entities. Potentially, they can exert tremendous control over third parties that use their platforms, giving them unique advantages in enforcement. But as we shall see, simply because tech giants have special capacity to monitor and police does not mean they have sufficient incentives to do so.

1.2 A Theory of Enforcer Compliance and Defiance

Why would big tech firms carry out enforcement tasks on behalf of the FTC? The simple answer is that they have a legal obligation to do so. But legal obligation does not necessarily lead to legal compliance, either in full or in part. The dynamic between the FTC and big tech enforcers resembles a classic principal-

agent relationship, where differences in goals, information, competency, and risks create conflicts between the two sides [10]. These conflicts reveal the many reasons why tech giants are likely to neglect their enforcement roles and allow third parties to violate consumer protections.

Fundamentally, the FTC and big tech have divergent, even irreconcilable interests. The FTC, as principal, has the primary goal of establishing effective oversight of online platforms in order to protect consumers and their privacy. But the combination of decentralization and rapid, bottom-up innovation makes the high-tech sector an especially difficult industry for the government to monitor [11]. Since the FTC cannot feasibly track the thousands of app development companies in the US, or the hundreds of thousands of independent developers, it needs to adopt efficient shortcuts that provide oversight of the digital economy at a low cost. The delegation of enforcement tasks accomplishes this goal. By ordering tech giants to police their own industry, the FTC can spend more time monitoring other commercial sectors and exert less effort in developing the necessary expertise to monitor high-tech firms.

But tech giants, as agents, have little or no interest in policing their business partners and would prefer to leave their platforms and networks unregulated for maximum profit [3]. Platform businesses, such as Apple, work to "bring together producers and consumers" with their mobile app stores and then rely on a high volume of exchanges to generate revenues [12, p. 58], see also [13]. They charge app developers a percentage of sales from the products sold on their app stores, and thus have a strong profit motive to increase the number of apps available to consumers. Meanwhile, social media companies, such as Facebook, sell access to their users' data—often for and through targeted advertising—to third parties. The more data that tech giants collect on their users, especially on highly sensitive activities, the more valuable their data and targeted ads are to companies and app developers [14]. Given how their businesses are structured, tech giants are likely to see third-party oversight as detrimental to their bottom lines.

The informational asymmetries that commonly exist between principals and agents operate between the FTC and big tech firms, providing further incentive for these firms to defy enforcement orders. Agency loss is a central problem for principals, since, generally speaking, agents have specialized knowledge and the means to withhold information for their own benefit [15]. One option in response is for principals to monitor agents directly, but doing so defeats the very purpose of delegating tasks [16, pp. 24–25]. Although the FTC has trained specialists to investigate tech companies, its workforce and budget are modest given its broad mission. For 2019, it had a $311 million budget and a staff of 1,100 to carry out all consumer investigations, in all commercial industries, not just those in the tech sector. Quite simply, the FTC often lacks the funds to launch major cases and finds itself outmatched by the army of lawyers and software engineers that these firms employ [17]. Tech giants likely realize that they can misrepresent their enforcement performance with little worry of the FTC catching on—especially because the government cannot readily recruit alternative enforcers to help overcome the asymmetries it faces in information and competency [18].

Moreover, the FTC faces graver potential consequences than tech firms do when enforcement failures occur, and this disparity in risks further incentivizes big tech to neglect oversight. Because of crisis or scandal, federal agencies can see their budgets cut, their mandates narrowed, and their leadership replaced or hallowed out [19]. Even an independent agency like the FTC—which, by design, is relatively insulated from political interference—can find itself targeted and penalized by politicians. In fact, political interference is increasingly common for such agencies [20]. The FTC has often found itself targeted by Congress over its regulatory performance, and legislators have threatened to shift oversight of the tech industry to other federal agencies [21], [22]. By contrast, tech giants face relatively miniscule fines for dropping the ball on enforcement and are unlikely to comply with FTC orders simply to avoid paying them. Fines in the tens of millions of dollars mean little to companies that earn hundreds of billions of dollars per year.

To return to our original question, why would tech giants comply with FTC orders when they have so many incentives and opportunities to defy them? We expect that these firms will only conduct third-party policing if the informational asymmetries between them and the FTC have been resolved, or at least dramatically reduced, and thus the threat of penalty for lapses has increased by a considerable degree. To be precise, tech firms will monitor business partners on a consistent basis if an alarm mechanism is in place that predictably and broadly exposes enforcement failures and in turn alerts the FTC. Not only does a consistent alarm raise the likelihood of government sanctions against delinquent enforcers, but also, and perhaps equally important, it raises public awareness of lapses and potentially triggers a public backlash against those enforcers that have allowed serious commercial abuses on their networks and platforms.

We see two sets of actors—consumers and the news media—playing a critical role in setting off alarms. When consumers lodge complaints against a third party for unfair or deceptive practices, the FTC learns that a

big tech enforcer has failed, to some extent, to monitor business partners; and when the news media covers such complaints, the FTC learns that the unfair or deceptive practices have been unusually severe, unusually widespread, or both. This kind of "fire alarm" mechanism, or "salience signal," has proved effective in ensuring regulatory action, oversight, and compliance in other contexts [23], [24], and we expect that it is likely to do so here. Specifically, if big tech enforcers know that consumers and the press will likely notice the deceptive practices of their business partners, they will have strong incentives to police their partners and quickly halt any deceptions or scams.

However, that also means tech giants can safely neglect oversight of third parties whose practices, even if highly problematic, are unlikely to be noticed by consumers or the news media. The absence of consumer complaints and news stories means the absence of an external alarm mechanism and thus little threat of investigation and public outrage.

2. Methods and Data Sources

In the remaining sections of this paper, we assess the plausibility of our enforcer theory against the empirical record. Specifically, we track the interactions between tech giants and the FTC to determine why companies followed or resisted government orders for third-party policing. Because firms have multiple opportunities to comply or defy and because the FTC has multiple opportunities to investigate and penalize, an examination of each company allows us to test our expectations repeatedly within cases and across time. An enforcer firm responds to an FTC request; the FTC responds to the performance of that firm; new business developments arise that create new enforcement demands, and so on. Given this ongoing dynamic, we use process-tracing methods to track causal mechanisms across time in order to explain the outcomes of interest: compliance and defiance of FTC orders [25], [26].

We examine two firms—Apple and Facebook—and thus construct two case studies to test our expectations. These companies, as part of the so-called Big Five tech giants, are directly comparable because they enjoy large revenues and market dominance in the same industry. In fact, not only do all three have considerable influence over app developers, but they also have the capacity to undermine, if not ruin, the fortunes of most developers simply by blocking access to their platforms or networks [27]. The FTC has imposed policing requirements on these companies for these reasons. Beyond these important similarities, we have decided to examine these firms because of two other considerations. First, and most important, these companies have demonstrated different levels of policing commitments and thus allow us to explore variation in the dependent variable. Second, these companies represent a mix of platform- and network-based businesses, with Apple offering platform services and Facebook offering network access. These companies thus represent the dominant business models that drive much of the high-tech sector [13]. However, despite variation in services and products across these firms, both showed initial resistance to third-party enforcement, suggesting that differences in business models do not account for differences in policing behavior.

The starting point for each case study is 2010—roughly when the FTC first investigated tech giants for compliance failures or recruited them for policing—and the timespan for each case encompasses the same ten-year period. By tracking firms over time, we can document not only their initial decisions to comply or defy but also their decisions to change behavior as a result of intervening events or shifting conditions. In using process tracing, we disaggregate each case into a series of salient episodes, see whether our causal mechanism is operating at each point in time, and determine whether its presence (or absence) has the hypothesized effect. Like Beach and Pedersen [28, p. 34] we understand a causal mechanism to be a series of "links" or a chain of related actions that lead to a particular result. That means the primary work of process tracing is to unpack those links—to isolate the actions—and demonstrate how each one contributes to the outcome of interest. As we have hypothesized, big tech firms will only comply with enforcement orders if they are convinced that an alarm mechanism that reliably notifies the FTC of enforcement failures is in place. Any alarm that alerts the FTC will alert the broad public by extension, potentially setting off a public backlash that will only strengthen the Commission's resolve to investigate and penalize.

We expect this alarm mechanism to unfold across four steps: users must recognize that a third party has committed abuses against them; users must then lodge public complaints against the third party, thus revealing enforcement lapses by the tech firm; these user complaints must receive at least some media attention to broaden awareness and spur government action; and the firm must plausibly expect additional user complaints to be registered and further, more serious government action to be taken unless it launches and maintains enforcement practices. If one link or more is missing, lapses in enforcement are likely to be observed, since tech giants will have few incentives to police third parties in a regulatory environment that they view as weak. Importantly, we do not argue or expect that the absence of an alarm mechanism will necessarily lead to the absence of FTC investigations. The agency conducts

periodic checks on its own, receives whistleblower complaints from company insiders, and sometimes assists other government agencies in their investigations. We simply expect that the absence of predictable alarms will encourage tech giants to defy FTC orders.

To construct our case studies, we draw upon multiple data sources—including government records, company statements, and press accounts, among others. Above all, we use materials from the FTC website, where the agency has compiled a full collection of enforcement orders, investigative records, consumer complaints, court judgments, and many other relevant documents pertaining to the tech firms. Our analysis is largely based on an exhaustive reading and appraisal of FTC files. The FTC provides detailed listings of all relevant case documents for both Apple (https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc) and Facebook (https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc). Having laid out our expectations and research strategies, we turn now to our case studies.

3. Apple

We begin our investigation with Apple and its initial failure to identify and block predatory sales practices on its app store. This case provides strong support for our main claim—that outside actors, especially consumers and the news media—play a critical role in establishing a predictable alarm system and holding enforcer firms accountable.

When Apple launched its app store in 2008, it focused on maximizing profits to the detriment of consumer protections. From the start, the company established its app store as the sole online marketplace for Apple customers to purchase applications for smartphones and tablets. The company also required app developers to pay 30% of their sales revenues to Apple in order to place their products on the app store. Apple claimed that its strict gatekeeping of apps was to ensure quality control, but this strategy also ensured that the company enjoyed large profits from the efforts and sales of app developers—about $5 billion a year [29]. To increase sales, Apple offered an in-app payment system that allowed users to download applications for free and buy optional, interactive features within the app itself. The in-app purchases were billed directly to the credit card associated with the device, speeding up transactions. However, Apple did not explain to customers how the new in-app purchasing system worked, nor did it set clear standards for app developers to follow for in-app offers. As a result, some app developers devised schemes to trick users into making unwanted in-app purchases [30].

Most problematic, some developers targeted children with this strategy. They created free videogames—known as "bait apps"—that allowed children to buy things, unknowingly, while they played online. Children would commonly need to purchase items, such as snacks for a virtual pet or additional chapters in a story, to reach successive levels in a game. Although parents had to enter an Apple password on their device for children to finalize these purchases, neither developers nor Apple made it clear to parents that, by punching in their passwords, they were authorizing a credit card charge. Moreover, Apple failed to warn parents that any use of their password would open a 15-minute window during which children could make unlimited in-app purchases without additional parental action. In one case, a child spent $2,600 on the game Pet Tap Hotel; in another, a seven-year-old spent $500 on the game Tiny Zoo Friends. Over the next several years, consumers reported millions of dollars of questionable in-app purchases to Apple and various authorities [30], [31].

An informal alarm system began to develop in 2010 and 2011 that brought public attention to children's bait apps and began to reduce the informational asymmetries between Apple and the FTC. Specifically, consumer complaints over in-app purchases drew the attention of the news media, which in turn drew the attention of legislators and regulators. Major outlets—including CBS News, the Associated Press, the *Washington Post*, and the comedy program *The Daily Show*—ran stories about parents receiving surprisingly large credit card bills because of their children's in-app purchases e.g. [32]–[34]. In response to these reports, three Democratic members of Congress formally requested that the FTC investigate platform providers and app developers for fraudulent practices [35]. Soon after, in early 2011, the FTC publicly announced that it would study the problem [36]. At the same time, disgruntled customers launched a class-action lawsuit against Apple in an effort to recover money from questionable app purchases [31].

Another important mechanism in the alarm system was added in 2012. That year, the FTC warned Apple and other tech firms that they needed to police third-party developers on their app stores and to notify parents of any purchasing schemes that targeted children. In a public report, the FTC explained that platform providers needed to consistently notify all users about interactive features in children's games. The agency noted that because Apple did not require third parties to inform customers in a clear, upfront manner, Apple was inviting and ultimately benefiting from predatory business practices. As the report explained, "This lack of enforcement provides little incentive to app

developers to provide such disclosures and leaves parents without the information they need. As gatekeepers of the app marketplace, the app stores should do more" [37, p. 3]. The report instructed tech giants—including Apple—to check whether apps on their platforms had interactive features and, where appropriate, to adopt warning measures that would prevent predatory or fraudulent in-app purchases.

Rather than follow the FTC's request, Apple continued its strategy of noncompliance and nonenforcement, allowing the problem of bait apps to worsen. While consumer complaints piled up, Apple claimed that it had no responsibility to provide clear terms of service as it defended itself against the class-action lawsuit [38]. With its first report having little perceivable impact, the FTC conducted another study of the app industry and issued a second report in late 2012. Not only did the FTC find that Apple had neglected its enforcement obligations over the last year, but it also concluded that predatory in-app purchases had likely increased. The agency found that, on Apple's platform, the proportion of children's games that offered in-app purchases had jumped from 11% to 30% in just ten months, making it all the more likely for children and parents to be duped into buying costly extras [39, p. 18]. This report concluded with a sharp warning to platform providers: "FTC staff has initiated a number of investigations to address the gaps between company practices and disclosures" [39, p. 21].

At this point it was clear to Apple that an alarm had fully sounded—that the public, the press, and government were committed to exposing abuses in the app industry. Apple thus took steps the following year to address customer complaints, clarify in-app purchasing procedures, and regulate its app store. In February 2013, it decided to settle the class-action lawsuit with disgruntled parents rather than continue its public denial of responsibility [40]. Two months later, it started to provide users with explanations on how in-app purchases worked and, in early 2014, it developed a clear warning system that notified parents about the 15-minute purchasing window each time a password was entered [30], [41]. These actions largely satisfied the FTC, but the agency took two additional steps to maintain pressure on Apple. First, it fined the company $32.5 million as compensation for affected customers and, second, it issued a standing, 20-year order that required Apple to continue the enforcement steps that it had already initiated [30].

From 2014 onward, Apple followed FTC orders and conducted scrupulous enforcement of its platform, avoiding further investigations. Apparently, the company recognized that neglect would set off a new wave of customer complaints, negative media reports, and thorough government investigations. In fact, having learned this lesson, Apple then developed smartphones with easy-to-use parental controls that allowed users to block all in-app purchases, further reducing the possibility of predatory schemes against children [42].

Table 1. Timeline of FTC investigation of Apple

Date	Event
Oct. 1, 2009	Apple introduces in-app payments (IAP).
Dec. 9, 2010	Nationally syndicated news article published about children accruing high bills for their parents through Apple's IAP [32]–[34].
Feb. 1, 2011	FTC investigation into IAP [36].
Mar. 2011	Growing consumer complaints about IAP, including class-action lawsuit. [30], [31].
Feb. 2013	Apple settles class-action lawsuit with parents [40].
Apr. 1, 2013	Apple displays on-device explanations about what IAPs are. Did not explain before this date [30], [37], [39].
Sep. 13, 2013	Further user interface changes made to clarify IAP process to consumers [30].
Jan. 15, 2014 - Mar. 27, 2014	Apple's agreement with the FTC was released and finalized.

4. Facebook

The case of Facebook presents clear evidence that corporate enforcement of third parties is repeatedly neglected when consumer complaints and other predictable sources of transparency are missing. When enforcer firms and their business partners can reliably conceal deceitful practices from the public and the press, they retain an informational advantage over the government and have little incentive to comply with FTC orders.

Facebook's enforcement lapse—allowing developers unauthorized and unregulated access to user data—was driven by profit motives. More than 98% of its revenues, roughly $70 billion a year, have come from advertising, especially from micro-targeted ads that appeal to narrow subsets of users [43]. For years, Facebook has collected profile information on its users—names, ages, locations, and any personal details shared with Facebook Friends, including educational attainment, work history, and political and religious views—in order to make perfect, or near-perfect, matches between users and ads. Initially, Facebook promised users that they could control access to their profile information and block third-party apps from collecting their data. But in December 2009, the company secretly changed settings that allowed third-

party apps to harvest data not only on a user who accessed their app, but also on all Friends in the user's network, i.e., "Affected Friends" [44].

Facebook's decision here revealed its willingness to take legal risks. Indeed, at the very same time that the company started misrepresenting its data policy, the FTC made enforcement of digital privacy a stated priority. In 2009, the Commission held roundtable discussions with experts—including Facebook representatives—to gain greater understanding of the issues at stake. Then, in 2010, it released a public report that highlighted its new investigative priorities and warned companies that their data-sharing practices needed to "comport with their representations to consumers" [45, p. 52]. The next year, the FTC completed an initial review of Facebook and found that the firm had secretly overridden privacy settings to let app developers harvest data on Affected Friends. To address this violation, the FTC issued a 20-year order that required Facebook to provide users with accurate explanations on how it shared data. The order also stipulated that Facebook would now need to "verify the privacy or security protections that any third party provides" once Facebook allowed data access [44]. That is, the tech giant would need to operate as an enforcer firm and conduct regular data-security audits on its business partners. What stands out from this episode is that, absent a clear alarm mechanism, Facebook operated without apparent concern for being investigated or caught.

Its new policing obligations, however, did not compel the company to change its behavior. In response to the FTC order, Facebook revised its privacy statement and alerted users that any data shared with Friends could be collected by third-party apps. But in 2012, just months after the FTC issued another, stronger order to Facebook, the company removed this disclaimer from its privacy policy while it still allowed third parties to access the data on Affected Friends [46]. It maintained third-party access, according to internal company records, because there was financial value in doing so. For example, apps that were denied access to user data tended to fail, thus cutting the number of products on Facebook and making the network less attractive to users [47].

Beyond profit motives, informational advantages over users and the government encouraged the company to commit willful misdeeds. In 2015, Facebook secretly allowed dozens of app developers to harvest Affected Friends data on a continuing basis, ensuring that tens of millions of users were unknowingly sharing their personal information. Facebook did not vet these developers or check whether they handled data responsibly [46]. Moreover, even when the company learned that an app developer was violating consumer privacy—say, by selling user data to an ad network—it made little or no effort to stop abuses. Typically, in such cases, a Facebook privacy manager would call an app developer to seek assurances, but otherwise would take no actions to ensure privacy standards were met [48]. Facebook founder Mark Zuckerberg specifically encouraged data sharing because he saw no risk of exposure. As he explained in a company email, "I think we leak info to developers but I just can't think of any instances where that data has leaked from developer to developer and caused a real issue for us"; quoted in [47]. Since the public and the government had no obvious means of learning how Facebook secretly shared personal data, the company had no inducements to conduct third-party oversight.

This neglect of enforcement led to the scandal over Cambridge Analytica, the British consulting firm that aided Donald Trump's first presidential campaign. In 2014, Cambridge Analytica offered to pay Facebook users a small sum to complete a personality test, ostensibly for academic research. After 270,000 people took the test, the company—contrary to FTC rules—gathered extensive personal data on roughly 87 million Affected Friends. Many of these Friends were outside the United States, but Cambridge Analytical had enough data on 30 million eligible voters in the US to micro-target ads in Trump's favor based on psychological profiles that the firm constructed [49], [50]. A little-noticed article on the company's activities was published in 2015, but Facebook—already aware of the campaign operation—took no enforcement steps in response [51]. Two tech-focused news sites ran stories on Cambridge Analytica after Trump's election win [52], [53], but again Facebook ignored its policing obligations. This is because the three reports, spaced fifteen months apart, failed to offer clear evidence of Facebook wrongdoing and therefore failed to mobilize the public or the FTC against the company. In fact, one story reported that "Cambridge Analytica [bought] personal data from a range of different sources" to develop its psychological profiles, and that it used the social media site simply to post ads [52]. An alarm was starting to sound at this point, but all the necessary components for an effective system—including public awareness of the relevant issues—were not yet in place to alter company behavior.

Facebook only adopted its enforcer role and suspended Cambridge Analytica's access to user data when a wave of news stories, based on insider accounts, revealed the depth of Facebook's data breaches. In March 2018, major news outlets, led by the *Washington Post* and the *New York Times*, ran detailed, investigative reports that exposed the widespread data access that Facebook had given Cambridge Analytica and other app developers. These news reports, dozens of them within

a month, raised serious public concerns and prompted both Congress and the FTC to launch investigations into Facebook's data-sharing practices [54], [55]. Only after these investigations were announced, and only after Facebook stocks plunged 8%, did Zuckerberg promise to rein in third-party access to user data [56]. To signal a commitment to enforcement, Facebook hired three highly regarded digital-rights advocates to work as privacy managers [57].

Thus, it took extensive news coverage, strong public reaction (including from investors), and a committed government response before the tech giant recognized that it could no longer shirk oversight and privacy responsibilities. The alarm had finally sounded. In 2019, to ensure that an alarm system remained in place, the FTC imposed an unprecedent $5 billion fine against Facebook and ordered the company to undergo an independent privacy audit each year, with the results to be made public [58]. Here, the FTC established a formal oversight system to ensure that secret company practices did not evade public scrutiny. Paradoxically, the Commission's plan was to rely on checks conducted by yet another set of agents to mitigate the problem of agency loss.

Table 2. Timeline of FTC investigation of Facebook

Date	Event
Dec. 1, 2009	Secretly changes user privacy settings that allow third parties to collect information contrary to privacy policy [44].
Dec. 2010	FTC issues report warning companies that all consumer data remain secure and private, consistent with any statements made to consumers [45].
Apr. 1, 2010	Facebook allows developers to collect data about Facebook App users and their friends ("Affected Friends").
Aug. 10, 2012	FTC orders Facebook to respect the privacy of users with mandated privacy reviews over 20 years [44]. Facebook alters privacy statement on web site to include disclaimer about sharing of data about friends [46].
Dec. 2012	Facebook removes disclaimer about sharing Affected Friends data [46].
Apr. 2014	Facebook claims that in a year no developer will have access to Affected Friends data [46].
Apr. 2015	Sharing of Affected Friends data continues with select developers [46].
Mar. 2018	Major US newspapers publish reports about how Cambridge Analytica was able to access data on 87 million Affected Friends based on a personality quiz taken by 270,000 people [49], [54], [55].
Jul. 24, 2019	Facebook was fined $5 billion by the FTC (23% of 2018's profits) [59].

5. Conclusions

Tech giants have an inconsistent record as enforcer firms. Both Apple and Facebook, as documented here, initially resisted FTC orders to stop app developers from making deceitful sales or violating user privacy. Pressure from the FTC eventually pushed Apple to police its app store, but similar pressure did not drive Facebook to protect user data. Why did Apple comply in full and Facebook not at all? In our view, the nature of third-party violations accounted for the differences in policing behavior. When app developers duped children into making in-app purchases, an informal alarm system quickly formed and alerted the FTC to enforcement failures. Disgruntled parents initially complained to Apple about questionable app charges, and when the tech giant ignored these complaints, parents sought help from news outlets. Stories about in-app purchasing schemes proliferated, pushing the FTC to investigate and ultimately fine Apple for negligent policing. Afterward, the company was motivated to conduct effective enforcement of its app store because any new consumer complaints would likely attract further press attention and sound the alarm again. By contrast, Facebook had no incentives to protect user data from third-party abuses because neither platform users nor the news media could discover the secret collection and mishandling of personal data. Since no alarm system could consistently ring for privacy violations, the tech giant allowed—and even encouraged—such violations to continue.

Our findings suggest that the FTC can only expect tech giants to conduct consistent and effective policing of third-party practices when consumer complaints are an ever-present threat. Without such a threat, the tech giants face no inducements to enforce government regulations and have strong reasons not to. Above all, third-party enforcement requires them to act against their business partners and, in turn, check their own profit opportunities. As we have shown, tech companies have violated user privacy not only because it is highly lucrative and central to their business models, but also because it is hard to expose. The FTC, in recent years, appears to have learned this lesson from the Facebook case and now requires this firm to undergo regular independent audits to compensate for a lack consumer and media alarms. It remains to be seen whether these independent audits will compel enforcer firms to uphold privacy laws and follow FTC orders over the long term.

6. References

[1] R. Van Loo, "The New Gatekeepers: Private Firms as Public Enforcers," *Va. Law Rev.*, vol. 106, p. 56, 2020.

[2] A. E. Waldman, "Privacy Law's False Promise," *Wash. Univ. Law Rev.*, vol. 97, no. 2, p. 62, Dec. 2019.

[3] S. Zuboff, "Big other: Surveillance Capitalism and the Prospects of an Information Civilization," *J. Inf. Technol.*, vol. 30, no. 1, pp. 75–89, Mar. 2015,

[4] E. Dal Bó, "Regulatory Capture: A Review," *Oxf. Rev. Econ. Policy*, vol. 22, no. 2, pp. 203–225, Jul. 2006,

[5] N. Gunningham, "Enforcement and Compliance Strategies," in *The Oxford Handbook of Regulation*, R. Baldwin, M. Cave, and M. Lodge, Eds. Oxford University Press, 2010, pp. 119–145.

[6] M. Moran, "Understanding the Regulatory State," *Br. J. Polit. Sci.*, vol. 32, no. 2, pp. 391–413, 2002.

[7] K. W. Abbott, D. Levi-Faur, and D. Snidal, "Theorizing Regulatory Intermediaries: The RIT Model," *Ann. Am. Acad. Pol. Soc. Sci.*, vol. 670, no. 1, pp. 14–35, Mar. 2017,

[8] C. J. Hoofnagle, *Federal Trade Commission privacy law and policy*. Cambridge University Press, 2016.

[9] A. Serwin, "The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices," *San Diego Law Rev.*, vol. 48, no. 3, p. 809, Aug. 2011.

[10] D. E. M. Sappington, "Incentives in Principal-Agent Relationships," *J. Econ. Perspect.*, vol. 5, no. 2, pp. 45–66, Jun. 1991,

[11] A. Thierer and B. Skorup, "A History of Cronyism and Capture in the Information Technology Sector," *J. Technol. Law Policy*, vol. 18, p. 131, 2013.

[12] M. W. V. Alstyne, G. Parker, and S. P. Choudary, "Pipelines, Platforms, and the New Rules of Strategy," *Harvard Business Publishing*, p. 8, Apr. 01, 2016.

[13] K. S. Rahman and K. Thelen, "The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism:," *Polit. Soc.*, Mar. 2019,

[14] S. C. Matz, M. Kosinski, G. Nave, and D. J. Stillwell, "Psychological targeting as an effective approach to digital mass persuasion," *Proc. Natl. Acad. Sci.*, vol. 114, no. 48, pp. 12714–12719, Nov. 2017,

[15] M. D. McCubbins, R. G. Noll, and B. R. Weingast, "Administrative Procedures as Instruments of Political Control," *J. Law Econ. Organ.*, vol. 3, no. 2, pp. 243–277, 1987.

[16] D. R. Kiewiet and M. D. McCubbins, *The Logic of Delegation*, 1st edition. Chicago: University of Chicago Press, 1991.

[17] L. Nylen, "FTC suffering a cash crunch as it prepares to battle Facebook," *POLITICO*, Dec. 10, 2020.

[18] K. W. Abbott, P. Genschel, D. Snidal, and B. Zangl, "Competence versus control: The governor's dilemma," *Regul. Gov.*, vol. 14, no. 4, pp. 619–636, 2020,

[19] K. A. Kemp, "Accidents, Scandals, and Political Support for Regulatory Agencies," *J. Polit.*, vol. 46, no. 2, pp. 401–427, May 1984,

[20] N. Devins and D. E. Lewis, "Not-So Independent Agencies: Party Polarization and the Limits of Institutional Design," *Boston Univ. Law Rev.*, vol. 88, p. 459, 2008.

[21] W. E. Kovacic and M. Winerman, "The Federal Trade Commission as an Independent Agency: Autonomy, Legitimacy, and Effectiveness," *Iowa Law Rev.*, vol. 100, p. 2085, 2015 2014.

[22] N. Scola and M. H. McGill, "Who should keep an eye on Silicon Valley?," *POLITICO*, Jul. 21, 2019.

[23] D. P. Carpenter, "Groups, the Media, Agency Waiting Costs, and FDA Drug Approval," *Am. J. Polit. Sci.*, vol. 46, no. 3, pp. 490–505, 2002,

[24] M. D. McCubbins and T. Schwartz, "Congressional Oversight Overlooked: Police Patrols versus Fire Alarms," *Am. J. Polit. Sci.*, vol. 28, no. 1, pp. 165–179, 1984,

[25] A. L. George and A. Bennett, *Case Studies and Theory Development in the Social Sciences*, Fourth Printing edition. Cambridge, Mass: The MIT Press, 2005.

[26] D. Beach and R. B. Pedersen, *Process-Tracing Methods*, 2nd ed. University of Michigan Press, 2019.

[27] R. Van Loo, "Federal Rules of Platform Procedure," Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3576562, Apr. 2020. https://papers.ssrn.com/abstract=3576562

[28] D. Beach and R. B. Pedersen, *Process-T-racing Methods*, 2nd edition. Michigan, USA: University of Michigan Press, 2019.

[29] K. Leswing, "Apple's App Store had gross sales around $50 billion last year, but growth is slowing," *CNBC*, Jan. 08, 2020.

[30] Federal Trade Commission, "Complaint. In the Matter of APPLE INC., a corporation.," Jan.

2014.https://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf
[31] C. Foresman, "Apple facing class-action lawsuit over kids' in-app purchases," *Ars Technica*, Apr. 16, 2011.
[32] Associated Press, "Apple App Store: Catnip for Free-Spending Kids?," *CBS News*, Dec. 9, 2010.
[33] C. Kang, "In-app purchases in iPad, iPhone, iPod kids' games touch off parental firestorm," *The Washington Post*, Feb. 08, 2011.
[34] K. C. Tofel, "My iTunes Account Was Hacked for $375 — By My Own Kids," *GigaOm*, Jul. 07, 2010.
[35] C. Kang, "Lawmakers urge FTC to investigate free kids games on iPhone," *The Washington Post*, Feb. 08, 2011.
[36] C. Kang, "FTC to review Apple iPhone in-app purchases," *The Washington Post*, Feb. 22, 2011.
[37] Federal Trade Commission, "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing," Feb. 2012. http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf
[38] V. Balasubramani, "Parents' Lawsuit Against Apple for In-App Purchases by Minor Children Moves Forward - In re Apple In-App Purchase Litigation," *Technology & Marketing Law Blog*, Apr. 11, 2012.
[39] Federal Trade Commission, "Mobile Apps for Kids: Disclosures Still Not Making the Grade," Federal Trade Commission, Dec. 2012. https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf
[40] J. Roberts, "Apple settles lawsuit over apps aimed at kids — will pay $5 iTunes credit or cash," *GigaOm*, Feb. 25, 2013.
[41] J. Clover, "iOS 7.1 Includes Warning Message About 15-Minute In-App Purchase Window," *MacRumors*, Mar. 12, 2014.
[42] B. X. Chen, "For Parental Controls, iPhones Beat Androids," *The New York Times*, Dec. 23, 2015.
[43] R. Iyengar, "Here's how big Facebook's ad business really is," *CNN*, Jul. 01, 2020.
[44] Federal Trade Commission, "Complaint In the Matter of FACEBOOK, INC., a corporation.," Federal Trade Commission, Nov. 2011. https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf
[45] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers," *J. Priv. Confidentiality*, Dec. 2010.
[46] Federal Trade Commission, "United States v. Facebook; Complaint for Civil Penalties, Injunction, and Other Relief," USDC, Case No. 19-cv-2184, Jul. 2019. https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf
[47] R. Cellan-Jones, "Facebook accused of 'secret data deals,'" *BBC News*, Dec. 05, 2018.
[48] S. Parakilas, "I worked at Facebook. I know how Cambridge Analytica could have happened.," *Washington Post*, Mar. 21, 2018.
[49] C. Kang and S. Frenkel, "Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users," *The New York Times*, Apr. 04, 2018.
[50] M. Rosenberg, N. Confessore, and C. Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions," *The New York Times*, Mar. 17, 2018.
[51] J. C. Wong, "Facebook acknowledges concerns over Cambridge Analytica emerged earlier than reported," *The Guardian*, Mar. 22, 2019.
[52] H. Grassegger and M. Krogerus, "The Data That Turned the World Upside Down," *Vice*, Jan. 29, 2017.
[53] M. Schwartz, "Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate," *The Intercept*, Mar. 30, 2017.
[54] T. Romm and C. Timberg, "FTC opens investigation into Facebook after Cambridge Analytica scrapes millions of users' personal information," *Washington Post*, Mar. 21, 2018.
[55] C. Timberg and T. Romm, "U.S. and British lawmakers demand answers from Facebook chief executive Mark Zuckerberg," *Washington Post*, Mar. 19, 2018.
[56] Associated Press, "Facebook's Zuckerberg apologizes for 'major breach of trust,'" *AP NEWS*, Mar. 22, 2018.
[57] E. Dreyfuss, "Facebook Hires Up Three of Its Biggest Privacy Critics," *Wired*, Jan. 30, 2019.
[58] Federal Trade Commission, "United States v. Facebook; Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief," USDC, Case No. 19-cv-2184, Jul. 2019. https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf
[59] J. Simons, N. J. Phillips, and C. S. Wilson, "Statement of Chairman Joe Simons and Commissioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc." Jul. 24, 2019.