International Journal of Law and Information Technology, 2022, **30**, 115–134
https://doi.org/10.1093/ijlit/eaac011
Advance access publication 8 September 2022
Article

OXFORD

Fox in the henhouse: The delegation of regulatory and privacy enforcement to big tech

William Bendix[*] and Jon MacKay[†]

ABSTRACT

The Federal Trade Commission (FTC) requires tech giants to identify and remove apps from their platforms that use deceitful sales tactics or violate user privacy. Tech giants have often resisted FTC orders because policing diminishes their profits. But while some firms have eventually complied with FTC demands, other firms have continued to shirk enforcement at the risk of escalating fines. What accounts for these different responses? Examining Apple, Google and Facebook, we find that tech giants willingly police consumer fraud but not consumer privacy violations. Failures to police fraud have led to public complaints and negative press attention, while failures to police data breaches often go undetected by users, the media and thus the FTC. We conclude that tech giants can act as effective regulatory agents on the government's behalf, but only when they police activities they cannot conceal.

KEYWORDS: FTC, tech giants, privacy, enforcer firms, regulation

INTRODUCTION

Overburdened as watchdogs, some federal agencies recruit industry-leading companies to conduct regulatory oversight on the USA 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 FTC has ordered tech giants to police the app developers that use their platforms

[*] Assistant Professor, Cyber Leadership and Intelligence, Dakota State University, Madison, SD, United States. Email: william.bendix@dsu.edu.
[†] Lecturer, Information Systems and Operations Management, Faculty of Business and Economics, The University of Auckland, Auckland, New Zealand. Email: jon.mackay@auckland.ac.nz.
[1] Rory Van Loo, 'The New Gatekeepers: Private Firms as Public Enforcers' (2020) 106 Virginia Law Review 467.

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.[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? What factors drive some big tech enforcers to conduct effective policing and others to let violations continue? To answer these questions, we examine three tech giants—Apple, Google and Facebook—and track their responses to FTC orders across a 10-year period, from 2010 to 2020. Initially, these companies 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. Google allowed the same type of fraudulent transactions, but went further and violated children's privacy to aid its business partners. 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; Google complied with some but not others; and Facebook committed ongoing policing failures.

These differences among the companies are puzzling because all three 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 even 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, Google 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. Publicly available documents, from both the US government and the companies, provide the necessary materials to assemble these case studies.

In the end, we find that the nature of violations was the decisive factor in determining whether tech giants willingly conducted enforcement. When parents reviewed billing statements and learned that their children had made unauthorized in-app purchases, many of them complained to Apple and Google 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. 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 Google and 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 two tech enforcers. 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.

For the remaining sections of this article, we proceed as follows. Next, we discuss the process by which the government recruits enforcer firms and the legal basis for the FTC to impose enforcement responsibilities on tech giants. We then discuss the principal-agent relationship that exists between the FTC and big tech enforcers, and we specify under what conditions these enforcers are likely to defy or comply with FTC policing orders. After discussing our empirical strategies and data sources, we present case-study evidence on Apple, Google and Facebook

[2] Ari Ezra Waldman, 'Privacy Law's False Promise' (2020) 97 Washington University Law Review 1; Van Loo (n 1).
[3] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

that supports our expectations. Finally, we conclude with a discussion on the implications of our findings, explaining how different business models that the tech giants have adopted will affect their willingness to comply with regulators over the long run.

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] 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'.[5]

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.[6] But violations short of complete delinquency are much harder for federal agencies to address. Because enforcer firms are not legally designated as state actors, they are not constrained by either the Administrative Procedures Act or the many court rulings that apply to federal regulators.[7] Their legally ambiguous position gives them the ability, potentially, to conduct enforcement in ways that enhance their own business interests.[8]

Enforcers in different industries—from banking to oil drilling—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.'[9]

[4] Ernesto Dal Bó, 'Regulatory Capture: A Review' (2006) 22 Oxford Review of Economic Policy 203; Neil Gunningham, 'Enforcement and Compliance Strategies' in Robert Baldwin, Martin Cave and Martin Lodge (eds), Neil Gunningham, *The Oxford Handbook of Regulation* (Oxford University Press 2010); Michael Moran, 'Understanding the Regulatory State' (2002) 32 British Journal of Political Science 391.

[5] Van Loo (n 1).

[6] Kenneth W Abbott, David Levi-Faur and Duncan Snidal, 'Theorizing Regulatory Intermediaries: The RIT Model' (2017) 670 The ANNALS of the American Academy of Political and Social Science 14; Van Loo (n 1).

[7] Administrative Procedure Act § 2, 5 U.S.C. § 551 (1994); Van Loo (n 1) 516–18.

[8] The Supreme Court has asserted that, in principle, the delegation of state authority onto private actors raises 'due process' concerns under the fifth and fourteenth amendments. Such delegation undermines the ability of affected third parties to seek full judicial remedy for problematic regulatory actions, since private surrogates, and not the executive itself, are responsible. Yet, in practice, the Supreme Court has frequently ruled against delegation challenges, allowing private actors to continue to operate on the government's behalf. The Court's record here has perplexed many observers. As Robbins explains, 'Commentators generally agree that the Supreme Court has not stated a satisfactory theory of the principles governing the delegation doctrine and has failed to articulate a precise test to distinguish between statutes that properly delegate and those that do not.' Refer Ira P Robbins, 'The Impact of the Delegation Doctrine on Prison Privatization' (1987) 35 UCLA Law Review 911, 921.

[9] Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

It also has the authority to investigate activities that potentially undermine consumer privacy, including online privacy.[10] Under these two broad mandates, the FTC has required the largest tech companies—including Apple, Google 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. Often, in these cases, the FTC adds oversight requirements to the standard checks that the tech giants already run before making such apps available. 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.[11]

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.[12] For tech giants, rather than monitoring surrogates, they police the use of their own networks, platforms and data by other entities—and do so often with the help of automated procedures—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.

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.[13] 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.[14] Since the FTC cannot feasibly track the thousands of app development companies in the USA, 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.[15] The delegation of enforcement tasks accomplishes this goal. By ordering tech giants to police their own

[10] Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (Cambridge University Press 2016); Andrew Serwin, 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices' (2011) 48 San Diego Law Review 809.

[11] Waldman (n 2); Van Loo (n 1).

[12] Van Loo (n 1) 490.

[13] David EM Sappington, 'Incentives in Principal-Agent Relationships' (1991) 5 Journal of Economic Perspectives 45.

[14] Adam Thierer and Brent Skorup, 'A History of Cronyism and Capture in the Information Technology Sector' (2013) 18 Journal of Technology Law & Policy 131.

[15] In 2020, the USA had roughly 7000 app development companies SoftwareWorld, 'Top 20+ Mobile App Development Companies USA' *SoftwareWorld*, (22 February 2021) <https://www.softwareworld.co/top-mobile-app-development-companies-in-usa/> accessed 22 February 2021.

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.[16] 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.[17] 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.[18] 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.[19] 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.[20] One option in response is for principals to monitor agents directly, but doing so defeats the very purpose of delegating tasks.[21] 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 1100 to carry out all consumer investigations, in all commercial industries, not just those in the tech sector.[22] 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.[23] 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.[24]

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.[25] Even an independent agency like the

[16] Zuboff (n 3).

[17] Marshall W Van Alstyne, Geoffrey Parker and Sangeet Paul Choudary, 'Pipelines, Platforms, and the New Rules of Strategy' (2016) 94 Harvard Business Publishing 8, 58; Refer also K Sabeel Rahman and Kathleen Thelen, 'The Rise of the Platform Business Model and the Transformation of Twenty-First-Century Capitalism': [2019] Politics & Society.

[18] Facebook has often claimed that it does not hand over data directly to third parties—that, instead, it simply makes ads available to Facebook users based on demographic features specified by advertisers. However, once users click on a targeted ad, companies learn that users fit within a highly targeted group, based on their personal data, social-network connections, and online activity. In short, advertisers know almost as much as Facebook does about a user. Michal Kosinski, 'Congress May Have Fallen for Facebook's Trap, but You Don't Have To' *The New York Times* (13 December 2018) <https://www.nytimes.com/2018/12/12/opinion/facebook-data-privacy-advertising.html> accessed 22 February 2021.

[19] SC Matz and others, 'Psychological Targeting as an Effective Approach to Digital Mass Persuasion' (2017) 114 Proceedings of the National Academy of Sciences 12714.

[20] Mathew D McCubbins, Roger G Noll and Barry R Weingast, 'Administrative Procedures as Instruments of Political Control' (1987) 3 Journal of Law, Economics, & Organization 243.

[21] D Roderick Kiewiet and Mathew D McCubbins, *The Logic of Delegation* (1st edn, University of Chicago Press 1991) 24–5.

[22] Refer Federal Trade Commission, 'FTC Appropriation and Full-Time Equivalent (FTE) History,' <https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation> accessed June 25, 2020.

[23] Leah Nylen, 'FTC Suffering a Cash Crunch as It Prepares to Battle Facebook' [2020] *POLITICO* <https://www.politico.com/news/2020/12/10/ftc-cash-facebook-lawsuit-444468> accessed 22 February 2021.

[24] Kenneth W Abbott and others, 'Competence versus Control: The Governor's Dilemma' (2020) 14 Regulation & Governance 619.

[25] Kathleen A Kemp, 'Accidents, Scandals, and Political Support for Regulatory Agencies' (1984) 46 The Journal of Politics 401.

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.[26] 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.[27] 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.

Beyond these features of the principal-agent relationship, one other factor likely encourages big tech enforcers to ignore enforcement orders. The FTC is best understood as a collective principal, not a unitary actor, and as such is vulnerable to divide-and-conquer strategies by agents.[28] Indeed, the FTC is led by five commissioners who, by majority vote, determine the agency's priorities and make final decisions over cases, penalties and settlements. Because a maximum of three commissioners may come from the same political party, the FTC is always led by a mix of Democrats and Republicans with differing views on consumer protections.[29] This split gives companies an opening to make targeted, ideological appeals to a narrow majority of commissioners, in an effort to discourage the agency from launching investigations or issuing fines. In fact, tech giants have adopted this strategy for years, hiring former FTC officials to lobby and negotiate with commissioners.[30] So even when tech firms cannot keep the FTC in the dark about enforcement failures, they can exploit the agency's political divisions to avoid or minimize penalties.

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,[31] and we expect that it is likely to do so here. Specifically,

[26] Presidents cannot remove appointed leaders from an independent agency. But increasingly, to weaken or punish such an agency, presidents leave leadership posts vacant. Refer Neal Devins and David E Lewis, 'Not-So Independent Agencies: Party Polarization and the Limits of Institutional Design' (2008) 88 Boston University Law Review 459, n 26.

[27] William E Kovacic and Marc Winerman, 'The Federal Trade Commission as an Independent Agency: Autonomy, Legitimacy, and Effectiveness' (2014) 100 Iowa Law Review 2085; Nancy Scola and Margaret Harding McGill, 'Who Should Keep an Eye on Silicon Valley?' *POLITICO*, (21 July 2019) <https://politi.co/2JGOx6w> accessed 16 July 2020.

[28] Kiewiet and McCubbins (n 21) 26–7.

[29] Kovacic and Winerman (n 27).

[30] For example, Google hired former FTC investigators to head off a preliminary antitrust probe in 2015. Company emails show that Robert Mahini, a former FTC official, oversaw Google's communications with the agency at that time (available at: <https://www.ftc.gov/system/files/documents/foia_requests/2015-00793commemailsapple-fb-google_0.pdf>) accessed March 23, 2022.

[31] Daniel P Carpenter, 'Groups, the Media, Agency Waiting Costs, and FDA Drug Approval' (2002) 46 American Journal of Political Science 490; Mathew D McCubbins and Thomas Schwartz, 'Congressional Oversight Overlooked: Police Patrols versus Fire Alarms' (1984) 28 American Journal of Political Science 165.

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.

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.[32]

We examine three firms—Apple, Google and Facebook—and thus construct three 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.[33] 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 and Google offering platform services and with Facebook offering network access. These companies thus represent the dominant business models that drive much of the high-tech sector.[34] However, despite variation in services and products across these firms, all three 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 10-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

[32] Derek Beach and Rasmus Brun Pedersen, *Process-Tracing Methods* (2nd edn, University of Michigan Press 2019); Alexander L George and Andrew Bennett, *Case Studies and Theory Development in the Social Sciences* (4th Printing edn, The MIT Press 2005).

[33] Rory Van Loo, 'Federal Rules of Platform Procedure' (Social Science Research Network 2020) SSRN Scholarly Paper ID 3576562 <https://papers.ssrn.com/abstract=3576562> accessed 9 July 2020.

[34] Rahman and Thelen (n 17) Amazon and Microsoft are the other two members that make up the Big Five. We do not include Amazon here because the details of its case—both the concerns over its app store and the company response to the FTC—are identical to those of Apple's case. The inclusion of Amazon would certainly reinforce our causal explanation, but space considerations prevent us from adding a fourth case. We do not include Microsoft simply because it has not received an enforcement order from the FTC and therefore does not qualify as an enforcer firm.

time, and determine whether its presence (or absence) has the hypothesized effect. Like Beach and Pedersen,[35] 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 is missing or more, 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 use the full collection of enforcement orders, investigative records, consumer complaints and court judgments, among other documents that the FTC website provides on the tech firms. Indeed, our analysis is largely based on an exhaustive reading and appraisal of these FTC files; and we rely heavily on the comprehensive and chronological listing of relevant case documents for Apple,[36] Google[37] and Facebook[38] that the agency has put together. We also use press accounts to supplement our analysis and to track public reactions to enforcement failures by the tech giants. For convenience, we include a timeline for each case to highlight major developments across our period of investigation (see Figures 1–3). Having laid out our expectations and research strategies, we turn now to our case studies.

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 per cent 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

[35] Beach and Pedersen (n 32) 34.
[36] Refer https://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc.
[37] Refer https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc.
[38] Refer https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

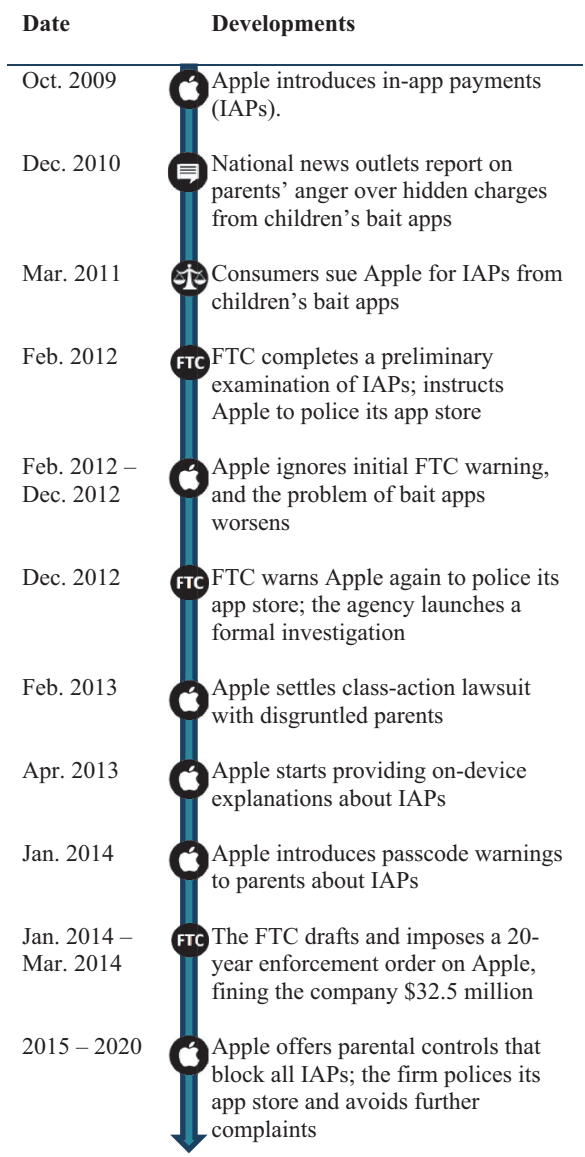

Figure 1. Timeline of Apple's Defiance and Compliance as an Enforcer Firm.

profits from the efforts and sales of app developers—about $5 billion a year.[39] 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

[39] Kif Leswing, 'Apple's App Store Had Gross Sales around $50 Billion Last Year, but Growth Is Slowing' *CNBC*, (8 January 2020) <https://www.cnbc.com/2020/01/07/apple-app-store-had-estimated-gross-sales-of-50-billion-in-2019.html> accessed 16 July 2020.

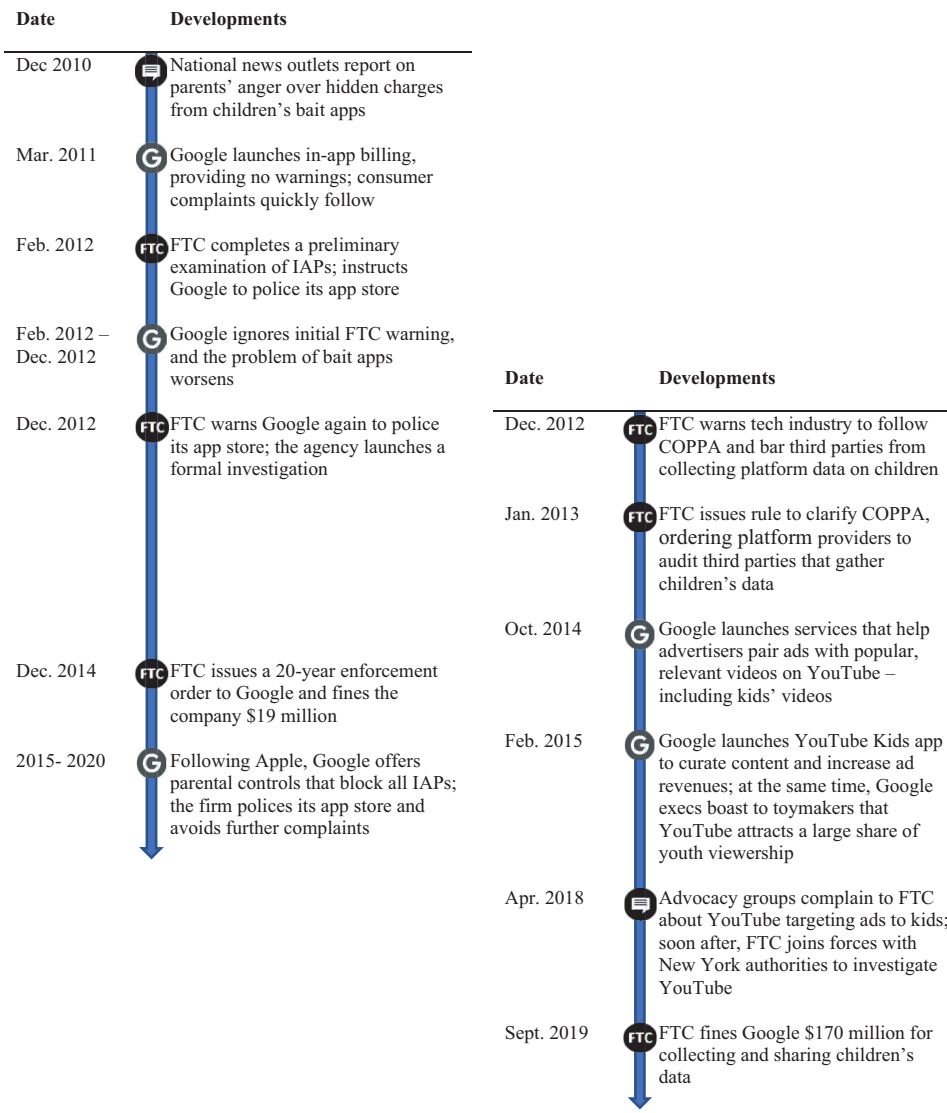

Figure 2. Timeline of Google's Defiance and Compliance as an Enforcer Firm.

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.[40]

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

[40] Federal Trade Commission, 'Complaint. In the Matter of APPLE INC., a Corporation.' (2014) <https://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf> accessed 17 March 2022.

Date	Developments
Dec. 2009	Facebook secretly changes user privacy settings that allow third parties to collect information contrary to its privacy policy
Dec. 2010	FTC warns platform providers that all consumer data remain secure and private, consistent with any statements made to users
Nov. 2011	FTC imposes 20-year order on Facebook, requiring it to make clear privacy statements and to police third parties that collect user data on its network
	Facebook updates privacy statement on its website
Aug. 2012	FTC issues another, stronger order to Facebook on policing duties
Dec. 2012	Facebook removes disclaimer about sharing Affected Friends data
Mid-2014	Cambridge Analytica pays 270,000 Facebook users to complete a personality test and gathers data on 87 million Affected Friends.
2015	Cambridge Analytica works with several Republican presidential candidates to micro-target ads, eventually working for Trump
Dec. 2015	The first news story on Cambridge Analytica and Facebook appears, but it receives little attention
Mar. 2018	Because of whistleblowers, major US news outlets report that Facebook and Cambridge Analytica violated the privacy of 87 million users to aid the Trump campaign
	Facebook suspends Cambridge Analytica's access to user data
Jan. 2019	Facebook hires three high-profile privacy officers
Jul. 2019	FTC fines Facebook $5 billion and imposes new privacy and compliance requirements on the company

Figure 3. Timeline of Facebook's Defiance and Compliance as an Enforcer Firm.

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 $2600 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.[41]

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.[42] In response to these reports, three Democratic members of Congress formally requested that the FTC investigate platform providers and app developers for fraudulent practices.[43] Soon after, in early 2011, the FTC publicly announced that it would study the problem.[44] At the same time, disgruntled customers launched a class-action lawsuit against Apple in an effort to recover money from questionable app purchases.[45]

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.'[46] 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.[47] With its first report having little perceivable impact, the FTC conducted another study of the app industry and issued a second report in

[41] Federal Trade Commission, 'Complaint. In the Matter of APPLE INC., a Corporation.' (n 40); Chris Foresman, 'Apple Facing Class-Action Lawsuit over Kids' in-App Purchases' *Ars Technica*, (16 April 2011) <https://arstechnica.com/gadgets/2011/04/apple-facing-class-action-lawsuit-over-kids-in-app-purchases/> accessed 12 July 2020.

[42] For Example Associated Press, 'Apple App Store: Catnip for Free-Spending Kids?' *CBS News*, (9 December 2010) <https://www.cbsnews.com/news/apple-app-store-catnip-for-free-spending-kids/> accessed 12 July 2020; Cecilia Kang, 'In-App Purchases in IPad, IPhone, IPod Kids' Games Touch off Parental Firestorm' *The Washington Post* (8 February 2011) <https://www.washingtonpost.com/wp-dyn/content/article/2011/02/07/AR2011020706073.html> accessed 14 July 2020; Kevin C Tofel, 'My ITunes Account Was Hacked for $375 — By My Own Kids' *GigaOm*, (7 July 2010) <https://gigaom.com/2010/07/07/my-itunes-account-was-hacked-for-375-by-my-own-kids/> accessed 14 July 2020.

[43] Cecilia Kang, 'Lawmakers Urge FTC to Investigate Free Kids Games on IPhone' *The Washington Post* (8 February 2011) <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/08/AR2011020805721.html> accessed 14 July 2020.

[44] Cecilia Kang, 'FTC to Review Apple IPhone In-App Purchases' *The Washington Post* (22 February 2011) <http://voices.washingtonpost.com/posttech/2011/02/ftc_chairman_to_probe_apple_ip.html> accessed 12 July 2020.

[45] Foresman (n 41).

[46] Federal Trade Commission, 'Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing' (2012) 3 <http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf> accessed 17 March 2022.

[47] Venkat 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*, (11 April 2012) <https://blog.ericgoldman.org/archives/2012/04/parents_lawsuit.htm> accessed 22 February 2021.

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 per cent to 30 per cent in just 10 months, making it all the more likely for children and parents to be duped into buying costly extras.[48] 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'.[49]

At this point it was clear to Apple that the public, the press and government were committed to exposing abuses in the app industry, and that an alarm had been fully sounded. 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.[50] 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.[51] 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.[52]

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.[53]

GOOGLE

Across the 10-year period that is the subject of our investigation, Google's activities also demonstrate that a predictable alarm, first sounded by disgruntled consumers, eventually leads to effective enforcement of third parties. But the case of Google—specifically its management of YouTube—reveals something more: that while a firm will act as an enforcer where consumer complaints loom, it will simultaneously abandon other policing responsibilities where no such complaints are likely to arise. In short, it will continue to exploit persistent informational asymmetries that allow it to act against the government's orders with little risk of getting caught.

Like Apple, Google had a legal responsibility to police children's games on its app store and, like Apple, it made no initial effort to do so. A relative latecomer to in-app purchasing, Google started processing such transactions in early 2011—when news reports had already exposed Apple's lack of enforcement. But the early alarms for Apple did not encourage Google to warn

[48] Federal Trade Commission, 'Mobile Apps for Kids: Disclosures Still Not Making the Grade' (Federal Trade Commission 2012) 18 <https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf> accessed 17 March 2022.

[49] 'Mobile Apps for Kids: Disclosures Still Not Making the Grade' (n 48) 21.

[50] Jeff Roberts, 'Apple Settles Lawsuit over Apps Aimed at Kids — Will Pay $5 ITunes Credit or Cash' *GigaOm*, (25 February 2013) <https://gigaom.com/2013/02/25/apple-settles-lawsuit-over-apps-aimed-at-kids-will-pay-5-itunes-credit-or-cash/> accessed 14 July 2020.

[51] Juli Clover, 'IOS 7.1 Includes Warning Message About 15-Minute In-App Purchase Window' *MacRumors*, (12 March 2014) <https://www.macrumors.com/2014/03/12/ios-7-1-in-app-purchase-warning/> accessed 16 July 2020; Federal Trade Commission, 'Complaint. In the Matter of APPLE INC., a Corporation.' (n 40).

[52] Federal Trade Commission, 'Complaint. In the Matter of APPLE INC., a Corporation.' (n 40).

[53] Brian X Chen, 'For Parental Controls, IPhones Beat Androids' *The New York Times* (23 December 2015) <https://www.nytimes.com/2015/12/24/technology/personaltech/for-parental-controls-iphones-beat-androids.html> accessed 22 February 2021.

parents about bait apps or possible in-app charges. In fact, Google made it even easier than Apple did for developers to trick children into buying extra features. The company required no passwords for in-app purchases and placed no time restrictions on them; once a 'free' app was downloaded, users could obtain additional interactive features without further approval. Almost immediately, Google started to receive customer complaints about unauthorized purchases—which led to the same kinds of news reports that had exposed Apple's wrongdoing.[54] But Google ignored concerns nonetheless; and it continued to do so even after the FTC, in early 2012, insisted that all platform providers issue clear, consistent warnings to parents about possible in-app charges. Only in late 2012, when the FTC announced investigations against both Apple and Google did the company finally require a password entry before processing in-app purchases. However, Google did not tell parents that, after entering their password, a 30-minute window opened in which children could make unlimited purchases. As a result, deceptive transactions continued.[55]

Following Apple's lead, Google only started to conduct effective oversight of its app store once it saw an alarm system fully in place. In late 2014, almost a year after the FTC had penalized Apple for enforcement failures, Google faced similar consequences. Along with a $19 million fine, the company received a 20-year order that required it to flag all games with in-app purchasing and to obtain consent from parents before processing any transactions.[56] To help meet its enforcement obligations, Google, in 2015, used Apple's strategy and developed parental controls for its Android devices that could block children from making any in-app purchases.[57] From that point on, Google provided clear markers for all games with in-app charges and avoided further government sanctions with regard to its app store. Presumably, it recognized that lapses in enforcement would trigger a swift, predictable sequence of consumer complaints, press reports and FTC investigations.

But simply because Google now had incentives to police its app store did not mean that it had incentives to police its other platform services. In 2012, when the FTC had warned tech giants to halt shady in-app purchases, the agency also instructed them to bar third parties from collecting online data on children.[58] It noted that such data-gathering practices violated the Children's Online Privacy Protection Act (COPPA).[59] The FTC took further action in 2013, issuing a rule that formally required all websites and platform providers to police children's privacy. The rule restated existing law that providers needed to obtain expressed consent from parents before collecting online data on children. The rule also stipulated that providers had to establish procedures for 'protect[ing] the confidentiality, security, and integrity of personal information collected from children'.[60] This rule required providers not only to take appropriate steps on children's data security themselves but also to make sure that any third parties that used their platforms did so as well. In practical terms, providers would need to audit the data-handling practices of third parties to meet federal regulations. For Google, this enforcement rule applied

[54] Anton Troianovski, Spencer E Ante and Jessica E Vascellaro, 'Mom, Please Feed My Apps!' Wall Street Journal (11 June 2012) <https://online.wsj.com/article/SB10001424052702303753904577452341745766920.html> accessed 23 March 2022; Brian Matt, 'Six Year Old Spends $149.99 On Android In-App Purchase' (TNW, 20 April 2011) <https://thenextweb.com/news/six-year-old-spends-149-99-on-android-in-app-purchase> accessed 23 March 2022.

[55] Federal Trade Commission, 'Complaint. In the Matter of Google, Inc.' (Federal Trade Commission 2014) 122 3237 1 <http://www.ftc.gov/system/files/documents/cases/141205googleplaycmpt.pdf> accessed 17 March 2022; Federal Trade Commission, 'Decision and Order. In the Matter of Google, Inc.' (Federal Trade Commission 2014) 122 3237 <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf> accessed 17 March 2022.

[56] Federal Trade Commission, 'Decision and Order. In the Matter of Google, Inc.' (n 55) 3.

[57] Chen (n 53).

[58] Federal Trade Commission, 'Mobile Apps for Kids: Disclosures Still Not Making the Grade' (n 48) 5.

[59] Children's Online Privacy Protection Act, 15 U.S. Code § 6502(a)(1).

[60] Federal Archives, 'Children's Online Privacy Protection Rule' (2013) 78 *Federal Register* 3972, 3995.

not only to its app store, but also to its other online services—including its video-sharing platform, YouTube.

But rather than conducting enforcement, Google and YouTube actively flouted privacy law to boost profits. YouTube generates most of its revenues—$15 billion in 2019 alone—from ad sales on videos.[61] It makes this money through partnerships with content providers who run monetized YouTube channels and upload free-to-view videos on the platform. The company monitors the online activities of viewers, selects ads based on their inferred preferences, and then shares ad profits with channel owners—an arrangement that encourages owners to upload increasingly popular videos for higher revenues.[62] With a standard terms-of-service agreement in place, such data-harvesting and ad-targeting schemes are permitted against adults—but not against children under COPPA and the FTC's 2013 rule. Yet for years YouTube tracked the viewing habits of children without parental permission, so that it could expose them to toy ads that matched their particular interests. Well beyond an enforcement failure, Google and YouTube actively broke the law to increase profits for third parties and themselves.

They likely committed these violations because they faced no obvious risk of detection. Since YouTube harvested data secretly, children and parents had no means of discovering the illegal collection and therefore had no basis for making public complaints that would alert federal regulators. A predictable alarm system could not develop under such conditions, all but ensuring that Google could increase child-directed content without penalty. In its sales presentations to Hasbro, Mattel and other toy companies, Google boasted that YouTube functioned as '[t]he new "Saturday Morning Cartoons"', and that it 'was unanimously voted as the favorite website for kids 2-12'. It even developed a YouTube Kids app to curate content based on different age groups. Yet, at the same time, Google assured channel operators that they did not need to comply with COPPA because, as one Google official claimed, 'we don't have users that are below 13 on YouTube'.[63] Such claims were, on their face, implausible, but they signaled to channel owners that Google had no commitment to privacy enforcement.

The company's brazen public statements likely reflected its perceived impunity in a marketplace without consumer alarms. But ultimately, these statements acted as the first triggers in a soon-to-emerge alarm system. In 2018, 23 advocacy groups submitted a report on YouTube's child programming to the FTC. The report documented the many public statements that Google and YouTube executives had made to advertisers about the popularity of children's content on their platform. The report also noted that YouTube had no separate privacy policy for children; the company merely provided a blanket warning that it deployed 'persistent identifiers to recognize a user over time and across different websites'.[64] Pointing to the centrality of children's videos on YouTube and the absence of a children's privacy policy, the report argued that the company was almost certainly tracking children online to target them with tailored ads. Evidently, the FTC found this report persuasive. Not only did it launch its own investigation against the company, but it also conducted a joint investigation with New York authorities against some YouTube channel owners.

[61] Dominic Rushe, '$15bn a Year: YouTube Reveals Its Ad Revenues for the First Time' *the Guardian* (3 February 2020) <http://www.theguardian.com/technology/2020/feb/03/youtube-ad-revenue-google-alphabet-shares> accessed 22 February 2021.

[62] Federal Trade Commission, 'Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief' (USDC 2019) 1:19-cv–2642 <https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_revised_complaint.pdf> accessed 6 July 2020.

[63] Federal Trade Commission, 'Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief' (n 62) 9.

[64] Angela J Campbell and Chris Laughlin, 'Request to Investigate Google's YouTube Online Service and Advertising Practices for Violating the Children's Online Privacy Protection Act' (Institute for Public Representation, Georgetown University Law Center 2018) Complaint 22 <https://default.salsalabs.org/T5b1625d0-3dc7-442d-bed9-28dc6e6e6e37/1df80f30-1641-11e8-8645-1252a0433360> accessed 17 March 2022.

The dual investigations led to penalties against Google and the establishment of a formal oversight system. In 2019, the FTC uncovered strong evidence of COPPA violations and fined Google $170 million. The Commission also imposed additional oversight tasks on Google, directing it to flag all channels that featured children's videos and requiring it to police YouTube channels for possible COPPA abuses. To verify its privacy efforts, Google would now need to submit compliance reports to the FTC and New York authorities for the next 10 years. It would also need to make employees available to government investigators for follow-up questioning upon request and without notice. The FTC also warned that additional compliance failures would lead to further legal action—including, potentially, criminal sanctions.[65] Apparently recognizing that secret data harvesting would trigger few or no public complaints, the FTC decided to establish its own monitoring and alarm system against such infractions in an effort to stem agency loss by Google.

FACEBOOK

The case of Facebook presents further 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 per cent of its revenues, roughly $70 billion a year, have come from advertising, especially from micro-targeted ads that appeal to narrow subsets of users.[66] 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, ie, 'Affected Friends'.[67]

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'.[68] 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

[65] Federal Trade Commission, 'Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief' (n 62).

[66] Rishi Iyengar, 'Here's How Big Facebook's Ad Business Really Is' *CNN*, (1 July 2020) <https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html> accessed 22 February 2021.

[67] Federal Trade Commission, 'Complaint in the Matter of FACEBOOK, INC., a Corporation.' (Federal Trade Commission 2011) 7 <https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf> accessed 17 March 2022.

[68] Federal Trade Commission, 'Protecting Consumer Privacy in an Era of Rapid Change–A Proposed Framework for Businesses and Policymakers' [2010] Journal of Privacy and Confidentiality 52 <http://www.journalprivacyconfidentiality.org/index.php/jpc/article/view/596> accessed 16 July 2020.

stipulated that Facebook would now need to 'verify the privacy or security protections that any third party provides' once Facebook allowed data access.[69] 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.[70] 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.[71]

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.[72] 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.[73] 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'.[74] 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 USA to micro-target ads in Trump's favor based on psychological profiles that the firm constructed.[75] A little-noticed article on the company's activities was published in

[69] Federal Trade Commission, 'United States v. Facebook; Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief' (USDC 2019) Case No. 19-cv-2184 13 <https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf> accessed 17 March 2022.

[70] Federal Trade Commission, 'United States v. Facebook; Complaint for Civil Penalties, Injunction, and Other Relief' (USDC 2019) Case No. 19-cv-2184 <https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf> accessed 17 March 2022.

[71] Rory Cellan-Jones, 'Facebook Accused of 'Secret Data Deals'' *BBC News* (5 December 2018) <https://www.bbc.com/news/technology-46456695> accessed 16 July 2020.

[72] Federal Trade Commission, 'United States v. Facebook; Complaint for Civil Penalties, Injunction, and Other Relief' (n 70) 5.

[73] Sandy Parakilas, 'I Worked at Facebook. I Know How Cambridge Analytica Could Have Happened.' *Washington Post* (21 March 2018) <https://www.washingtonpost.com/opinions/i-worked-at-facebook-i-know-how-cambridge-analytica-could-have-happened/2018/03/20/edc7ef8a-2bc4-11e8-8ad6-fbc50284fce8_story.html> accessed 16 July 2020.

[74] Quoted in Cellan-Jones (n 71).

[75] Cecilia Kang and Sheera Frenkel, 'Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users' *The New York Times* (4 April 2018) <https://www.nytimes.com/2018/04/04/technology/mark-zuckerberg-testify-congress.html> accessed 16 July 2020; Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, 'How Trump Consultants Exploited the Facebook Data of Millions' *The New York Times* (17 March 2018) <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> accessed 16 July 2020.

2015, but Facebook—already aware of the campaign operation—took no enforcement steps in response.[76] Two tech-focused news sites ran stories on Cambridge Analytica after Trump's election win,[77] but again Facebook ignored its policing obligations. This was 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.[78] 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.[79] Only after these investigations were announced, and only after Facebook stocks plunged 8 per cent, did Zuckerberg promise to rein in third-party access to user data.[80] To signal a commitment to enforcement, Facebook hired three highly regarded digital-rights advocates to work as privacy managers.[81]

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 unprecedented $5 billion fine against Facebook and ordered the company to undergo an independent privacy audit each year, with the results to be made public.[82] Here, as it had done with Google and YouTube, 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.

[76] Julia Carrie Wong, 'Facebook Acknowledges Concerns over Cambridge Analytica Emerged Earlier than Reported' *The Guardian* (22 March 2019) <https://www.theguardian.com/uk-news/2019/mar/21/facebook-knew-of-cambridge-analytica-data-misuse-earlier-than-reported-court-filing> accessed 16 July 2020.

[77] Hannes Grassegger and Mikael Krogerus, 'The Data That Turned the World Upside Down' *Vice*, (29 January 2017) <https://www.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win> accessed 16 July 2020; Mattathias Schwartz, 'Facebook Failed to Protect 30 Million Users From Having Their Data Harvested by Trump Campaign Affiliate' *The Intercept*, (30 March 2017) <https://theintercept.com/2017/03/30/facebook-failed-to-protect-30-million-users-from-having-their-data-harvested-by-trump-campaign-affiliate/> accessed 16 July 2020.

[78] Grassegger and Krogerus (n 77).

[79] Tony Romm and Craig Timberg, 'FTC Opens Investigation into Facebook after Cambridge Analytica Scrapes Millions of Users' Personal Information' *Washington Post* (21 March 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/03/20/ftc-opens-investigation-into-facebook-after-cambridge-analytica-scrapes-millions-of-users-personal-information/> accessed 16 July 2020; Craig Timberg and Tony Romm, 'U.S. and British Lawmakers Demand Answers from Facebook Chief Executive Mark Zuckerberg' *Washington Post* (19 March 2018) <https://www.washingtonpost.com/news/the-switch/wp/2018/03/18/u-s-and-british-lawmakers-demand-answers-from-facebook-chief-executive-mark-zuckerberg/> accessed 16 July 2020.

[80] Associated Press, 'Facebook's Zuckerberg Apologizes for 'Major Breach of Trust'' *AP NEWS*, (22 March 2018) <https://apnews.com/c8f615be9523421998b4fcc16374ff37> accessed 16 July 2020.

[81] Emily Dreyfuss, 'Facebook Hires Up Three of Its Biggest Privacy Critics' [2019] *Wired* <https://www.wired.com/story/facebook-hires-privacy-critics/> accessed 16 July 2020.

[82] Federal Trade Commission, 'United States v. Facebook; Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief' (n 69).

CONCLUDING DISCUSSION

Tech giants have an inconsistent record as enforcer firms. All of them, 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 and Google to police their app stores, but similar pressure did not drive Google or Facebook to protect user data. Why did Apple comply in full, Google in part 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 and Google about questionable app charges, and when the tech giants 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 and Google for negligent policing. Afterward, the two companies were motivated to conduct effective enforcement of their app stores because any new consumer complaints would likely attract further press attention and sound the alarm again. By contrast, Google and 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 giants 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 Google-YouTube and Facebook cases, and now requires these enforcer firms to undergo regular independent audits where no consumer and media alarm exists.

We expect that the relative secrecy by which tech firms operate will continue to determine whether they defy or comply with regulators. But we recognize that their ability to operate in secret will be determined largely by the business models these companies have already adopted; moreover, these differences in business models will only set the companies further apart as they decide whether to follow, oppose or even subvert government regulators in the USA and elsewhere.

Apple, for example, cannot operate its app store in secret, nor can it conceal controversies over the way it manages its platform from policymakers or the public. Recently, the most successful app developers on Apple's platform have taken the company to court over what they describe as anti-competitive practices.[83] Policymakers in Europe,[84] South Korea[85] and the United States[86] have all noticed, launching investigations into the company's management of its app store. Furthermore, the European Union has drafted legislation that would impose

[83] Tim Higgins, 'Apple's Fight for Control Over Apps Moves to Congress and EU' *Wall Street Journal* (23 June 2021) <https://www.wsj.com/articles/apples-fight-for-control-over-apps-moves-to-congress-and-eu-11624440601> accessed 19 March 2022.

[84] Sam Schechner and Tim Higgins, 'Apple's Hold on App Store Set to Face Significant Challenge from New European Law' *Wall Street Journal* (17 March 2022) <https://www.wsj.com/articles/apples-hold-on-app-store-set-to-face-significant-challenge-from-new-european-law-11647520201> accessed 19 March 2022.

[85] Jiyoung Sohn, 'Google, Apple Hit by First Law Threatening Dominance Over App-Store Payments' *Wall Street Journal* (31 August 2021) <https://www.wsj.com/articles/google-apple-hit-in-south-korea-by-worlds-first-law-ending-their-dominance-over-app-store-payments-11630403335> accessed 19 March 2022.

[86] Ryan Tracy, 'App-Store Bill Targeting Apple, Google Is Approved by Senate Panel' *Wall Street Journal* (3 February 2022) <https://www.wsj.com/articles/app-store-bill-targeting-apple-google-is-approved-by-senate-panel-11643910888> accessed 19 March 2022.

staggering fines—up to 10 per cent of a company's global revenues—for engaging in the kinds of business practices that Apple now uses to run its app store.[87] For Apple, its platform accounts for about 20 per cent of its annual operating income, but the firm remains largely a technology hardware company that uses its app store to lure users into purchasing Apple products.[88] So even though it continues to challenge regulatory efforts in court over app-store operations, its long-run concern is to minimize such disputes and concentrate on maintaining a large share of the smartphone and tablet market.

Facebook, at the other extreme, depends on collecting and monetizing user data from its social network, and can still engage in relatively secret data-handling practices despite the independent audits it now faces. With 98 per cent of its total annual revenues coming from advertising, it simply cannot afford to curtail data sharing in order to comply with FTC requirements.[89] One continued tactic of the company's is to change privacy settings frequently in the hope that most users fail to update these settings and thus leave their data open for third parties to exploit.[90] Recent reports on a variety of other blatant violations by Facebook show that the company has no immediate interest in reforming its ways.[91]

One final point needs to be highlighted. In establishing independent audits to ensure that firms like Facebook remain committed to privacy enforcement, the FTC has delegated oversight yet again and has avoided doing direct oversight itself. Who watches the watchers? Apparently, another set of watchers and not the FTC. Granted, government regulators often institute and rely on fire alarms as their main means of oversight, as opposed to conducting police patrols themselves, because this strategy offers principals an efficient way to monitor many agents.[92] But the FTC's reliance on several layers of delegated enforcers suggests that the agency is massively overburdened and severely under-resourced. It would be hardly surprising, then, if tech giants continued to flout FTC orders.

[87] Schechner and Higgins (n 84).

[88] Schechner and Higgins (n 84).

[89] Rishi Iyengar, 'Here's How Big Facebook's Ad Business Really Is' *CNN*, (1 July 2020) <https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html> accessed 22 March 2022.

[90] Heather Kelly, 'Facebook Privacy Settings to Change Now' *Washington Post* (23 September 2021) <https://www.washingtonpost.com/technology/2021/09/23/facebook-privacy-settings/> accessed 20 March 2022.

[91] Jeff Horwitz, 'Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt.' Wall Street Journal (13 September 2021) <https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353> accessed 21 October 2021; Jeff Horwitz, 'The Facebook Whistleblower, Frances Haugen, Says She Wants to Fix the Company, Not Harm It' Wall Street Journal (3 October 2021) <https://www.wsj.com/articles/facebook-whistleblower-frances-haugen-says-she-wants-to-fix-the-company-not-harm-it-11633304122> accessed 21 October 2021; Jeff Horwitz and Keach Hagey, 'Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.' *Wall Street Journal* (15 September 2021) <https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215> accessed 21 October 2021.

[92] McCubbins and Schwartz (n 31).