National Security by Platform

Elena Chachko*

25 STAN. TECH. L. REV. 55 (2021)

ABSTRACT

Since 2016, platforms like Facebook, Google and Twitter have scaled up their efforts to meet a plethora of security and geopolitical challenges. They have gradually recalibrated their organizational structures and practices for that purpose. The challenges include election security, disinformation and influence operations, foreign and domestic terrorism, and atrocity prevention worldwide. As a corollary, platforms have expanded their interaction with government around these issues. They have also replicated traditional government methods for addressing them. Existing law facilitates this relationship instead of meaningfully constraining it.

Scholars have examined platform governance predominantly through a freedom of expression lens. The security and geopolitical aspects of platform governance, however, remain surprisingly undertheorized. This article shifts the focus from platform speech governance to platform security governance. It documents platforms' geopolitical turn and how it shapes the public-private

* Rappaport Fellow, Harvard Law School; Fellow, The Miller Institute for Global Challenges and the Law, University of California, Berkeley School of Law; echachko@law.harvard.edu. I am grateful to Scott Anderson, Julian Arato, Yochai Benkler, Gabby Blum, Kathleen Claussen, Ashley Deeks, Yoav Dotan, Evelyn Douek, Kristen Eichensehr, Andrew Gold, Jack Goldsmith, Jon Gould, Ben Heath, Chris Hoofnagle, Maryam Jamshidi, Ido Kilovaty, Steve Koh, Jeff Kosseff, Katerina Linos, Orly Lobel, Asaf Lubin, Jon Michaels, Omer Netzer, Gali Racabi, Daphna Renan, Alan Rozenshtein, Oren Tamir, Rebecca Wexler, Christopher Yoo, Diego Zambrano, participants of the 2021 Cybersecurity Law and Policy Scholars Conference, the faculty workshop at the University of San Diego Law School, and former tech executives who requested to remain anonymous for invaluable comments and conversations. Finally, I thank the exceptional *Stanfrod Technology Law Review* editorial team. This project benefitted from the generous support of Perry World House, University of Pennsylvania, where I was a 2019 Global Order Fellow.

national security nexus. It argues that platforms' growing security and geopolitical role is a novel mode of informal national security privatization—call it national security by platform—that deviates in form and substance from paradigmatic privatization models. The paper develops a theoretical framework for analyzing national security by platform and outlines preliminary implications for regulation. The security lens illuminates regulatory considerations that may conflict with speech, competition and privacy concerns that have dominated the platform regulation debate to date.

TABLE OF CONTENTS

I. INTRODUCTION

Major technology companies including Facebook, Google, Twitter, and Microsoft issued a series of joint statements ahead of the 2020 U.S. election. Those brief boilerplate readouts were products of an election integrity working group comprising industry leaders and U.S. government agencies.[1] Cooperation between industry and government tightened as election day approached. Platform officials on mushrooming "trust and safety" teams repeatedly highlighted the importance of close coordination with the FBI and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to secure the election.[2]

While collaborating with government agencies, platforms countered a White House campaign to discredit the election results. Despite past reluctance to do so, Twitter, Facebook (now Meta) and others famously deplatformed former President Trump for inciting violence in the aftermath of the January 6 capitol riots. They also sanctioned domestic militia groups and individuals.[3]

---

[1] *See, e.g.*, Facebook Newsroom (@fbnewsroom), *Joint Industry Statement on Ongoing Election Security Collaboration Between Tech Companies and USG Agencies Tasked with Protecting the Integrity of the Election*, TWITTER (Aug. 12, 2020, 3:31 PM), https://perma.cc/CV8F-6H8S. According to the companies, "[f]or the past several years, we have worked closely to counter information operations across our platforms." *Id. See* discussion *infra* Part II.A.

[2] *See* sources cited *infra* notes 68, 97. Platform officials even publicly praised CISA's head for his role in securing the election after President Trump fired him. *See* Nathaniel Gleicher (@ngleicher), TWITTER (Nov. 17, 2020, 7:39 PM), https://perma.cc/HMP2-H8CB.

[3] *See* Twitter Inc., *Permanent Suspension of @realDonaldTrump*, TWITTER BLOG (Jan. 8, 2021), ("After close review of recent Tweets from the @realDonaldTrump account and the context around them—specifically how they are being received and interpreted on and off Twitter—we have permanently suspended the account due to the risk of further incitement of violence."); Kate Conger & Mike Isaac, *Inside Twitter's Decision to Cut Off Trump*, N.Y. TIMES (Jan. 16, 2021), https://perma.cc/Z9NP-KEKN; Guy Rosen & Monika Bickert, *Our Response to the Violence in Washington*, FACEBOOK NEWSROOM (Jan. 6, 2021), https://perma.cc/5P37-H4WN ("Over the last several years, we have allowed President Trump to use our platform consistent with our own rules, at times removing content or labeling his posts when they violate our policies. . . . But the current context is now fundamentally different, involving use of our platform to incite violent insurrection against a democratically elected government.

Although essentially labeling the U.S. President a national security threat was unprecedented, blocking accounts for security reasons had by then become a common platform practice worldwide.[4]

On another front, platforms have ramped up their capacity to address global conflicts. For example, Facebook formed a Strategic Response Team in the aftermath of the 2017 Myanmar atrocities[5] and the company's contribution to violence in global hot spots elsewhere.[6] Members of the team have "experience in foreign affairs or conflict situations."[7] Its leader has said that "[t]here's a lot of similarities there between government and military and Facebook."[8] Platforms have been embroiled in the Taliban takeover of

---

We believe the risks of allowing the President to continue to use our service during this period are simply too great." (quoting Mark Zuckerberg, FACEBOOK (Jan. 7, 2021, 10:47 AM))); Ben Collins (@oneunderscore_), TWITTER (Jan. 8, 2021, 4:19 PM), https://perma.cc/NY4L-KH7M; Ahiza García-Hodges, Ben Collins & Dylan Byers, *Facebook and Twitter Lock Trump's Accounts After Posting Video Praising Rioters*, NBC NEWS (Jan. 6, 2021), https://perma.cc/8J2J-U9JX; *see also* Genevieve Lakier & Nelson Tebbe, *After The "Great Deplatforming": Reconsidering the Shape of the First Amendment*, LPE PROJECT (Mar. 1, 2021), https://perma.cc/8PEU-33XV.

These actions set off a cascade of deplatforming by other companies. *See* First Draft (@firstdraftnews), TWITTER (Jan. 12, 2021, 3:25 PM), https://perma.cc/YT8K-YHUZ (aggregating platform responses to the events of January 6).

[4] *See infra* Parts II.B and III.B.

[5] Hum. Rts. Council, Rep. of the Independent International Fact-Finding Mission on Myanmar, UN Doc. A/HRC/39/64, at 14 (2018), https://perma.cc/4KPZ-46UF ("The role of social media is significant. Facebook has been a useful instrument for those seeking to spread hate, in a context where, for most users, Facebook is the Internet. Although improved in recent months, the response of Facebook has been slow and ineffective. The extent to which Facebook posts and messages have led to real-world discrimination and violence must be independently and thoroughly examined."); BSR, HUMAN RIGHTS IMPACT ASSESSMENT: FACEBOOK IN MYANMAR (2018); Kevin Roose & Paul Mozur, *Zuckerberg Was Called Out Over Myanmar Violence. Here's His Apology*, N.Y. TIMES (Apr. 9, 2018), https://perma.cc/7RD5-FDH9.

[6] Amanda Taub & Max Fisher, *Where Countries Are Tinderboxes and Facebook Is a Match*, N.Y. TIMES (Apr. 21, 2018), https://perma.cc/T6NP-ULCV.

[7] David Ingram, *Facebook's New Rapid Response Team Has a Crucial Task: Avoid Fueling Another Genocide*, NBC NEWS (June 20, 2019), https://perma.cc/CRD6-RCDP.

[8] *Id.* Facebook appears to have learned from the 2017 Myanmar episode. Following the military coup in the country in 2021, Facebook banned military-affiliated accounts from the platform. *See* Nathaniel Gleicher (@ngleicher), TWITTER (Feb. 24, 2021, 11:04 PM), https://perma.cc/RYJ6-J4WL; Paul Mozur, Mike Isaac, David E. Sanger & Richard C. Paddock, *Facebook Takes a Side, Barring Myanmar Military After Coup*, N.Y. TIMES (updated Mar. 3, 2021), https://perma.cc/6CWX-8XFK.

Afghanistan following the U.S. withdrawal,[9] geopolitical conflict in India,[10] the recent military coup in Myanmar,[11] and violence in Gaza and Israel.[12] They have operated elections and conflict "war rooms."[13] Facebook, for one, now has about 40,000 people working on trust and safety.[14] The entire U.S. foreign service numbers roughly 15,600.[15]

These are but a few illustrations of a significant recent phenomenon. Leading technology platforms—Facebook, Google, Twitter, and increasingly other companies[16]—have gradually recalibrated their organizational structures, policies and practices to better meet geopolitical and security challenges incidental to their business operations. The challenges include counterterrorism and both foreign and domestic violent extremism, election integrity, influence operations and other harmful disinformation, global conflicts, related interactions with governments, and other tasks that we typically associate with national foreign and security bureaucracies and think of as government responsibilities.[17] As a corollary, increased platform

---

[9] *See* Cristiano Lima, *The Technology 202: Facebook, Twitter, YouTube Face High-Stakes Question of Whether to Recognize Taliban*, WASH. POST (Aug. 17, 2021), https://perma.cc/AM4H-7NUL; Diksha Madhok, *How Social Media Is Dealing with the Taliban Takeover*, CNN (Aug. 17, 2021), https://perma.cc/2YQB-32YN.

[10] Jeff Horwitz, *Facebook Blocks, Then Restores, Content Calling on Indian Prime Minister Modi to Resign*, WALL ST. J. (Apr. 28, 2021), https://perma.cc/8DJH-UKYG.

[11] Jenny Domino, *Beyond the Coup in Myanmar: The Other De-Platforming We Should Have Been Talking About*, JUST SECURITY (May 11, 2021), https://perma.cc/7ZGM-MSAU.

[12] Elizabeth Culliford, *Facebook Deploys Special Team as Israel-Gaza Conflict Spreads Across Social Media*, REUTERS (May 19, 2021), https://perma.cc/EUR4-4LW5.

[13] *See infra* Part II.

[14] *See infra* Part II.B.1.

[15] Julie Nutter, *The Foreign Service by the Numbers: Where We Stand*, FOREIGN SERV. J., Jan.-Feb. 2020, at 60. As of 2019, the State Department employed a total of 77,243 employees. *See* U.S. DEP'T OF STATE BUREAU OF HUM. RESOURCES, HR FACT SHEET (Mar. 31, 2019), https://perma.cc/K4L7-5F8V.

[16] *See supra* note 3 and accompanying text.

[17] I am not committing to any single definition of security or geopolitics here. Suffice it to say that both these terms have been defined broadly in scholarship and practice. For instance, global threat assessments from the Office of the Director of National Intelligence in recent years have addressed not only traditional challenges such as state adversaries, terrorism, and weapons of mass destruction, but also human security, public health, and climate change. *See, e.g.*, DANIEL R. COATS, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY (2019); *see also, e.g.*, J. Benton Heath, *Making Sense of Security,* AM. J. INT'L L. (forthcoming 2022); J. Benton Heath, *The New National Security Challenge to the Economic Order,* 129 YALE L.J. 924, 1029 (2020); Laura K. Donohue, *The Limits of National Security*, 48 AM. CRIM. L. REV. 1573, 1706–09 (2011).

engagement with security and geopolitics has created a complex government-platform nexus in those areas.

Scholars have examined platform governance predominantly through a freedom of expression lens.[18] Despite their growing significance, the

---

[18] Kate Klonick's influential work dubbed major Internet platforms like Facebook, Google, Twitter, and Amazon "The New Governors." Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech,* 131 HARV. L. REV. 1598 (2018) [hereinafter Klonick, *The New Governors*]. However, the geopolitical and security aspects of platform governance have not inspired robust scholarly attention to date. Scholars have intensely debated platforms' extraordinary power to regulate speech, their control over modern civil discourse, and their role in facilitating the spread of misinformation and disinformation. *See*, *e.g.*, *id.*; SOCIAL MEDIA AND DEMOCRACY: THE STATE OF THE FIELD AND PROSPECTS FOR REFORM (Nathaniel Persily & Joshua A. Tucker eds., 2020) (surveying related literature); Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45 (2020); Jack M. Balkin, *Old-School/New-School Speech Regulation,* 127 HARV. L. REV. 2296 (2014); Danielle Keats Citron & Helen L. Norton, *Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age*, 91 B.U. L. REV. 1435 (2011); ROBERT M. FARIS ET AL., BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y, PARTISANSHIP, PROPAGANDA, AND DISINFORMATION: ONLINE MEDIA AND THE 2016 U.S. PRESIDENTIAL ELECTION (2017).

Scholars have also extensively analyzed platforms' evolving content moderation policies and oversight mechanisms. *See, e.g.*, Klonick, *The New Governors, supra*; Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418 (2020) [hereinafter Klonick, *The Facebook Oversight Board*]; Evelyn Douek*, What Kind of Oversight Board Have You Given Us?,* U. CHI. L. REV. ONLINE (May 11, 2020), https://perma.cc/DX83-QN4Q; Daphne Keller, *Platform Content Regulation—Some Models and Their Problem*s, THE CTR. FOR INTERNET AND SOC'Y (May 6, 2019), https://perma.cc/EE4L-FH7H. This has called for the need for "platform separation of powers" in forming policy and adjudicating disputes. *See, e.g.*, Rory Van Loo, *Federal Rules of Platform Procedure*, 88 U. CHI. L. REV. 829 (2021). Additional work analyzes platforms' contribution to government surveillance and law enforcement. *See, e.g.*, Ashley Deeks, *Secrecy Surrogates,* 106 VA. L. REV. 1395 (2020); Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance,* 72 VAND. L. REV. 1563 (2019); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018); Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security & Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473 (2016). Another line of work addresses platforms' overwhelming market power. *See, e.g.*, FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH (2017); JONATHAN TAPLIN, MOVE FAST AND BREAK THINGS: HOW FACEBOOK, GOOGLE, AND AMAZON CORNERED CULTURE AND UNDERMINED DEMOCRACY (2017); MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016); Thomas Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951 (2021); Lina M. Khan, *The Separation of Platforms and Commerce,* 119 COLUM. L. REV. 973 (2019) [hereinafter Khan, *Separation of Platforms*]; Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017); Lina M. Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017) [hereinafter Khan, *Amazon's Antitrust Paradox*]. Finally, scholars have discussed whether platforms are capable of overpowering and displacing sovereigns. *See*, *e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A

geopolitical and security aspects of platform governance and platforms' role in the modern public-private security ecosystem remain surprisingly undertheorized.[19]

This paper shifts the focus from platform speech governance to platform security governance. It argues that key elements of the evolving government-platform relationship around security and geopolitics constitute indirect and informal privatization—call it *national security by platform*. It is privatization in the fundamental sense that private actors perform core traditional government functions.[20] But national security by platform also deviates from paradigmatic theoretical understandings of privatization as deliberate government delegation to private actors anchored in a legal instrument.[21] It is not typically initiated by a formal legal arrangement, there is no subject matter or geographic restriction on the scope of privatized functions, and government is not the gatekeeper. The paper theorizes this novel mode of national security privatization and considers its implications.

Part II of the paper examines platforms' geopolitical turn. It documents the emergence of geopolitical and security organizational structures, policies, and procedures within major platforms and their functions. This account is based on official platform data and a comprehensive analysis of policy documents, journalistic and scholarly accounts, and informal statements by platform trust and safety and public policy officials.

Focusing on the United States, Part III then analyzes the part-symbiotic, part-adversarial emerging platform-government relationship around core national security and geopolitical matters. The relationship involves both direct cooperation and platforms independently replicating government national

---

BORDERLESS WORLD (2006); Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665 (2019); Andrew Keane Woods, *Aegis Paper Series No. 1813*, *Tech Firms are Not Sovereigns,* HOOVER INST. (2018). This paper complements these debates by providing an integrated account of the geopolitical and security aspects of platform operations, turning the focus to what is taking place behind the screens.

[19] *But see, e.g.*, GOLDSMITH & WU, *supra* note 18; Eichensehr, *supra* note 18; Woods, *supra* note 18. For an early influential analysis of "the invisible handshake" between government and private technology companies in counterterrorism, see Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment,* 8 VA. J. L. & TECH. (2003).

Even if one thinks of it as little more than window dressing driven by political and business expediency, platforms' geopolitical turn and the related government-platform interface are significant developments that merit exploration.

[20] *See infra* Part III.B.

[21] *Id.*

security and foreign policy practices. Part II shows that ambient law—constitutional, statutory, and judicial—facilitates and even incentivizes this government-platform national security relationship.

Part IV frames national security by platform as a novel form of informal privatization and examines how it deviates from paradigmatic theoretical understandings of privatization. I build on important contributions by Kristen Eichensehr and Jon Michaels,[22] whose work begins to explore new modes of national security privatization in cybersecurity and counterterrorism. I propose a typology of circumstances in which informal de facto delegation of national security responsibilities to platforms may occur: (1) *hard structural constraints on government*—constitutional and institutional—in addressing threats that play out in privately controlled theaters; (2) *bureaucratic workarounds*, meaning informal reliance of government actors on platforms as their long arm in handling certain issues for political or pragmatic reasons even when government has authority and institutional competence to act directly; and (3) *platforms as substitutes*, that is, instances in which platforms openly defy the government's explicit position, or supplant government because government ceded the territory due to indecision, neglect, or lack of interest.[23]

The first two categories involve a cooperative government-platform dynamic. The third category covers unilateral platform action. The second and third category are contingent. The government-platform relationship in those categories depends on the degree of political and policy alignment among the legislature, the Executive, the administrative state, and platforms. By contrast, the first category covers inevitable cooperation driven by hard constraints on government. It is thus less susceptible to political and policy shifts.[24] It is likely to endure even as government contemplates adverse regulatory action against platforms like reforming Section 230 of the Communications Decency Act.[25]

Part V builds on this theoretical framework and considers preliminary regulatory implications. The security lens adds a new facet to a platform regulation conversation that has so far been dominated by speech, privacy, and

---

[22] *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467 (2017); Jon D. Michaels, *Deputizing Homeland Security*, 88 TEX. L. REV. 1435 (2010) [hereinafter Michaels, *Deputizing Homeland Security*]; Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Gathering in the War on Terror*, 96 CALIF. L. REV. 901 (2008) [hereinafter Michaels, *All the President's Spies*].

[23] *See infra* Part IV.A.

[24] *See infra* Part IV.A.4.

[25] 47 U.S.C. § 230; *see infra* Part III.C.

competition interests. It highlights certain regulatory concerns that may conflict with those interests, and it focuses attention on the government-platform relationship.

For example, scholars have criticized cooperative, informal government-platform arrangements like the election security working group and the Global Internet Forum to Counter Terrorism (GIFCT) on freedom of expression grounds.[26] But such soft institutional arrangements might be an effective second-best approach in the category of hard structural constraints. They are a substitute for binding regulation made difficult by current interpretations of the First Amendment. They help platforms and government compensate for institutional deficits in addressing platform-enabled security and geopolitical challenges, and they may facilitate a degree of mutual accountability.[27]

In the category of bureaucratic workarounds, relying on private actors to end-run law and procedure could drive *government* foreign and security action further beyond the reach of Congress and the courts. The government-platforms dynamic here augments already broad executive national security authorities to blacklist individuals and groups and to acquire data. As a first step, this category therefore calls for greater constraints on informal government reliance on platforms to eschew law, process, and oversight.[28] The category of platforms as substitutes invites discussion of avenues available to the federal government to undercut platform action when it contradicts U.S. security or geopolitical interests.[29]

Finally, there is tension between security and competition concerns in platform regulation. Platform size and global market dominance might be an advantage from a national security vantage point. The fewer players are involved in policing and responding to online threats, the easier it should be for government to build partnerships and coordinate public-private responses. Government-platform security cooperation therefore complicates recent government antitrust action against platforms.[30]

Two caveats are in order. First, there is ample reason to doubt the effectiveness of platforms' new geopolitical and security policies and related organizational changes in meeting the challenges for which they were

---

[26] *See infra* Part V.A.

[27] *See id.*

[28] *See infra* Part V.B.

[29] *See infra* Part V.C.

[30] *See infra* Part V.D.

ostensibly designed.[31] There is also reason to doubt that platforms are capable of meeting those challenges, or that they prioritize security and user well-being over profit. Indeed, critics have argued that platforms' new policies and reforms are little more than an elaborate public relations stunt—window dressing to deflect public criticism and appease regulators.[32] Recognizing this, the aim of my analysis is not to grade platform security and geopolitical performance. Rather, the aim is to understand and theorize platforms' security and geopolitical functions with an emphasis on the platform-government relationship in these areas.

Second, this paper focuses on the United States. Platforms have performed unevenly on security and geopolitical matters in other parts of the world.[33] The legal underpinnings of the theoretical framework developed here and the normative calculus in assessing government-platform cooperation are context dependent. They could therefore be different in countries with other regime types and public law systems.

---

[31] Information that came to light recently about Facebook makes it abundantly clear that the company repeatedly falls short in preventing its products from causing harm and prioritizes profit over safety. The same applies to other platforms as well. *See, e.g.*, *Protecting Kids Online: Testimony from a Facebook Whistleblower Before the Subcomm. On Consumer Prot., Prod. Safety, and Data Sec. of the Sen. Comm. on Com., Sci., & Transp.*, 116th Cong. (2021); Ryan Mac & Sheera Frenkel, *Internal Alarm, Public Shrugs: Facebook's Employees Dissect Its Election Role*, N.Y. TIMES (Oct. 23, 2021), https://perma.cc/6VPR-QKU2; Craig Silverman, Ryan Mac & Pranav Dixit, *"I Have Blood on My Hands": A Whistleblower Says Facebook Ignored Global Political Manipulation*, BUZZFEED NEWS (Sept. 14, 2020), https://perma.cc/MQ6J-MJK4 ("[T]he failures . . . observed during her two-and-a-half years at the company [in the whistleblower's belief were not] the result of bad intent by Facebook's employees or leadership. It was a lack of resources . . . and the company's tendency to focus on global activity that posed public relations risks, as opposed to electoral or civic harm."); Olivia Solon, *Counter-Terrorism Was Never Meant to be Silicon Valley's Job. Is That Why It's Failing?*, GUARDIAN (June 29, 2017), https://perma.cc/WJ2P-DHDQ ("'It's all bullshit. It's an effort to generate a veneer of corporate responsibility for the benefit of their shareholders that is frankly anything but that' . . . . [T]ech companies 'understand the issues' but have 'about a one-inch deep knowledge of a two-mile deep pond of centuries-old issues.").

[32] *See* sources cited *supra* note 31.

[33] *See, e.g.*, the sources cited *supra* note 31; *see also* Rebecca Hamilton, *De-platforming Following Capitol Insurrection Highlights Global Inequities Behind Content Moderation*, JUST SEC. (Jan. 20, 2021), https://perma.cc/9YH9-XHYS; Alaphia Zoyab, *Silicon Valley's Double Standard*, REST WORLD (Jan. 25, 2021), https://perma.cc/A9DF-T49D; Adam Satariano, *After Banning Trump, Facebook and Twitter Face Scrutiny About Inaction Abroad,* N.Y. TIMES (Jan. 17, 2021), https://perma.cc/6HBP-T5MH; Justin Scheck, Newley Purnell & Jeff Horwitz, *Facebook Employees Flag Drug Cartels and Human Traffickers. The Company's Response Is Weak*, *Documents Show*, WALL ST. J. (Sept. 16, 2021), https://perma.cc/QS6S-7E97 ("Facebook has focused its safety efforts on wealthier markets with powerful governments and media institutions . . . even as it has turned to poorer countries for user growth.").

National security by platform has emerged in an ad hoc fashion around high-profile events such as elections, sectarian violence, and terrorist attacks without much consideration of the broader questions raised by platform performance of core national security and geopolitical functions. This paper brings those issues to the forefront. It develops privatization theory to capture national security by platform as part of the modern public-private national security nexus. The analysis should be of interest to scholars of the new post-2016 world of platform governance, privatization theorists, and scholars of foreign affairs and national security power.

II. PLATFORMS' GEOPOLITICAL TURN

What, precisely, is new about the relatively recent increase in platform engagement with security and geopolitics? What precipitated it? What were the major organizational shifts within platforms that accompanied it? This Part documents what I call platforms' geopolitical turn, marking the year 2016 as a critical juncture. Part III then turns to the geopolitical and security platform-government nexus.

A. From Business Diplomacy to Global Security at Scale

Platforms have been leading something akin to private foreign policies for a while now. In 2011, an article entitled "Facebook Diplomacy" described a new Facebook initiative to create a team of foreign policy directors—"ambassadors"—to represent the company in relations with foreign governments.[34] "The move," according to the article, "has been characterized as a new, private-sector type of Foreign Service."[35] Google reportedly created a similar program as early as 2006.[36] Facebook's CEO, Mark Zuckerberg, "has so frequently met with world leaders—as sort of a peer, as Facebook's large global audience gives him a hefty constituency in many lands—that people commonly refer to the company's 'foreign policy.'"[37]

---

[34] Chrisella Sagers, *Facebook Diplomacy*, DIPLOMATIC COURIER (June 8, 2011), https://perma.cc/KCX5-4LD7; *see also* David Kirkpatrick, *Does Facebook Have a Foreign Policy?*, 190 FOREIGN POL'Y 55 (2011).

[35] Sagers, *supra* note 34.

[36] *Id.*

[37] STEVEN LEVY, FACEBOOK: THE INSIDE STORY 6 (2020). Foreign countries have even sent their own ambassadors to Silicon Valley. Upon his appointment to the post, the Danish ambassador

This sort of international advocacy is not in itself surprising for influential transnational corporations like Facebook, Google and other major platforms. After all, the United Fruit Company, Exxon Mobil, BP, Coca-Cola and McDonalds—to name only a few influential transnational corporations—have long functioned as important geopolitical actors with infamous international risk management and lobbying apparatuses.[38] The fact that large technology companies perform security and geopolitical functions and develop relevant organizational infrastructure is therefore a predictable artifact of platforms' growth and global influence.

Nevertheless, certain platform features and the kinds of products that they offer make their geopolitical and security role unique compared to more traditional transnational corporations and other forms of private actor participation in security and geopolitics.[39] Platforms are in constant interaction

---

tasked with representing his government's interests before the likes of Google and Facebook said that "[t]hese companies have moved from being companies with commercial interests to actually becoming de facto foreign policy actors." *See* Adam Satariano, *The World's First Ambassador to the Tech Industry*, N.Y. TIMES (Sept. 3, 2019), https://perma.cc/KH87-9WTL.

[38] On the geopolitical and risk assessment aspects of transnational corporations, see, for example, STEVE COLL, PRIVATE EMPIRE: EXXON MOBIL AND AMERICAN POWER (2012); and PETER CHAPMAN, BANANAS: HOW THE UNITED FRUIT COMPANY SHAPED THE WORLD (2007); *see also* Adalberto J.S. Fernandes et al., *Managing Political Risk in the Oil and Gas Industry in a Developing Economy: The Case of BP in Angola*, 13 EUR. J. OF INT'L MGMT. 733 (2019); Megan Quek & Tapan Sarker, *Transnational Corporations in the Extractive Industries Operating in Conflict States: How Far Should Corporate Citizenship Extend?*, 44 J. OF CORP. CITIZENSHIP 29 (2011); Deborah Avant, *NGOs, Corporations and Security Transformation in Africa*, 21 INT'L RELATIONS 143 (2007).

[39] Other examples include the proliferation of private national security contractors, addressed in Part III.B. In addition, financial institutions have created compliance mechanisms to implement proliferating security and geopolitics-driven financial regulation. Since 9/11, they have had to build institutional capacity to contend with an economic sanctions boom, counterterrorism and other anti-money laundering requirements, ever expanding export control lists and more. *See, e.g.*, GIBSON DUNN, ANTI-MONEY LAUNDERING AND SANCTIONS ENFORCEMENT AND COMPLIANCE IN 2020 AND BEYOND (2020), https://perma.cc/3GUS-WX5E; GREGORY HUSISIAN, FOLEY & LARDNER LLP, COPING WITH U.S. REGULATION OF INTERNATIONAL CONDUCT: COMPLIANCE STRATEGIES FOR THE FOREIGN CORRUPT PRACTICES ACT, EXPORT CONTROLS, SANCTIONS, AND ANTI-MONEY LAUNDERING LAWS AND REGULATIONS 1 (2009), https://perma.cc/3EY7-7V9Z ("In recent years, the U.S. Government has become increasingly aggressive in enforcing U.S. laws designed to regulate the conduct of U.S. citizens and companies operating abroad. As a result, multinational firms face multiplying compliance concerns, especially with regard to the Foreign Corrupt Practices Act, export control and sanction regulations, and anti-money laundering requirements."). Finally, private actors are also increasingly required to meet certain cybersecurity standards, partially in response to damaging high profile cyberattacks against U.S. targets by foreign nations like China and Russia. *See* Exec. Order 14028, Improving the Nation's Cybersecurity, 86 Fed. Reg. 26,633, § 2 (May 17, 2021).

with billions of users worldwide and have certain regulatory power over them.[40] They are omnipresent and inherently public-facing. We interact with dominant multinationals like Shell or Toyota a handful of times per month at most. Compare that to our daily direct and indirect interaction with Google, Facebook, Instagram, WhatsApp, or Twitter. Platforms exercise significant control over global information flows. They operate in a particularly large number of countries. Almost every significant geopolitical development in the world, from elections to violent conflict, is relevant to their operations. They must be vigilant about a breathtaking spectrum of threats from multiple sources at once and engage in constant enforcement. This is a much larger and more diverse scale of geopolitical influence and interests compared to even the most historically powerful traditional transnational corporations.[41]

What is more, the geopolitical and security functions of major platforms in the last few years—while undoubtedly driven by self-interest [42] —have expanded dramatically. Major platforms have moved far beyond advocacy with foreign governments centered on traditional business goals, such as steering local regulation to protect narrow corporate interests, advancing new business, or protecting global physical assets and employees.

---

[40] *See* Jack M. Balkin, *Free Speech Is a Triangle*, 118 COLUM. L. REV. 2011 (2012) (framing twenty-first century speech regulation as a competitive triangular system comprising government, speakers, and private speech regulators, and highlighting the complex private governance system created by social media companies and their bureaucracies).

[41] *See also* Eichensehr, *supra* note 18, at 667-68 ("To be sure, these are not the first superempowered private parties, but they differ in some salient ways from other powerful private actors, both historical and contemporary . . . . They aspire to be global, not national. They have global users, not just customers or shareholders. And they are attractive, not extractive, drawing on soft power rather than hard power.").

[42] It would not be a stretch to speculate that this development has been driven in substantial part by self-interest and a need to respond to public and political pressure and preserve legitimacy—"trust" in common tech parlance—among users. The motives behind these reforms are not crucial for my analysis, which takes the emergence of these organs as the point of departure and considers their structural implications. *See, e.g.*, KNIGHT FOUNDATION & GALLUP, TECHLASH? AMERICA'S GROWING CONCERN WITH MAJOR TECHNOLOGY COMPANIES 1 (2020), https://perma.cc/LA6A-RZQM ("Gallup's tracking of public sentiment toward the internet industry shows a decline from a high of 60% of Americans with positive views of such companies in 2015 to 43% of Americans viewing them positively and 30% viewing them negatively in 2019—up 14 percentage points from 2015."); Rana Foroohar, *Year in a Word: Techlash*, FIN. TIMES (Dec. 16, 2018), https://perma.cc/9MNF-9TFE ("This year will be remembered as the moment big tech faltered.").

A series of events around 2016 marked a turning point in how major platforms interact with the global and security environment.[43] Key among those developments was the role of major platforms in facilitating the spread of disinformation during the 2016 U.S. election, including the Russian effort to undermine the process.[44] But the election was hardly the only catalyst for change. Around the same time, Facebook was accused of contributing to the spread of violence in global hot spots like Myanmar, Thailand, and Sri Lanka.[45] Platform exploitation by transnational terrorist and violent extremist groups such as ISIS and Al-Qaeda—which platforms had already acted against at that point[46]—and by domestic actors in various countries received heightened scrutiny as well.[47]

---

[43] *See* sources cited *supra* note 42; *see also, e.g.*, Nick Clegg, *New Facebook and Instagram Research Initiative to Look at US 2020 Presidential Election*, FACEBOOK NEWSROOM (Aug. 31, 2020), https://perma.cc/G6Q8-Q8HB ("This research is part of Facebook's wider effort to protect elections. As a company, we've looked hard at what went wrong with Russian interference in 2016 and made some big changes."); *Are We Ready? Foreign Interference, Disinformation, and the 2020 Election,* ATL. COUNCIL (Aug. 25, 2020), https://perma.cc/B59D-H42P [hereinafter *Atlantic Council Panel*] (transcript on file with the author) (remarks by Nathaniel Gleicher, Head of Security Policy, Facebook) ("I think in 2016, if you look across the communities that you need to defend against influence operations, by and large, we weren't ready. We didn't see it coming."); *see also* LEVY, *supra* note 37, at 10-12.

[44] *See* OFF. OF THE DIR. OF NAT'L INTEL., ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT U.S. ELECTIONS ii (2017), https://perma.cc/ZSA2-FT5N ("Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations . . . with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or 'trolls.'"); ROBERT S. MUELLER, III, OFF. OF SPECIAL COUNS., 1 REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14-35 (2019), https://perma.cc/6G48-8AQU; U.S. SEN. SELECT COMM. ON INTEL., 116TH CONG., RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION: VOLUME 2: RUSSIA'S USE OF SOCIAL MEDIA, WITH ADDITIONAL VIEWS (2019), https://perma.cc/6GLK-BME8; *see also, e.g.*, FARIS ET AL., *supra* note 18; Cecilia Kang, Nicholas Fandos & Mike Isaac, *Tech Executives Are Contrite About Election Meddling, but Make Few Promises on Capitol Hill*, N.Y. TIMES (Oct. 31, 2017), https://perma.cc/C458-T6NY (quoting Twitter's General Counsel: "The abuse of our platform to attempt state-sponsored manipulation of elections is a new challenge for us—and one that we are determined to meet"); Moira Whelan, *It's Time for the State Department to Stop Throwing Money at Facebook*, FOREIGN POL'Y (Oct. 31, 2017), https://perma.cc/4XTM-ANU5 ("The use of social media by foreign agents to destabilize the 2016 U.S. presidential election has received increasing attention over the past few months.").

[45] *Supra* notes 5-6.

[46] *Infra* note 116.

[47] *See infra* note 153 and accompanying text; *see also, e.g.*, HOME AFFS. COMM., HATE CRIME: ABUSE, HATE AND EXTREMISM ONLINE, 2016-17, HC 609, ¶ 24 (UK) ("It is shocking that Google failed to perform basic due diligence regarding advertising on YouTube paid for by reputable

These events provoked a barrage of political, regulatory, and public pressure on platforms to address the negative geopolitical and security effects of their products and services.[48] Platforms were no longer able to credibly present themselves as neutral facilitators of speech and benevolent agents of social organization[49] or place responsibility for any adverse outcomes with users. They were forced to contend with the oft-destructive impact of misinformation, disinformation, incitement, and viral amplification of content within their domain.[50]

Consequently, industry leaders like Facebook, Google, and Twitter—to varying degrees—have gradually adopted a more proactive approach to defending their platforms and products against a variety of threats and threat actors. These threats include the erosion of election integrity, influence operations, foreign and domestic violent extremism, incitement to violence and terrorism, sectarian conflict worldwide, and public safety challenges related to COVID-19.[51]

---

companies and organisations which appeared alongside videos containing inappropriate and unacceptable content, some of which were created by terrorist organisations. We believe it to be a reflection of the laissez-faire approach that many social media companies have taken to moderating extremist content on their platforms."); Scott Shane, *In 'Watershed Moment,' YouTube Blocks Extremist Cleric's Message*, N.Y. TIMES (Nov. 12, 2017), https://perma.cc/7ULG-M7WM.

[48] *See* LEVY, *supra* note 37, at 11.

[49] For more on Facebook's universalist standard aspirations, see Monika Bickert, *Defining the Boundaries of Free Speech on Social Media*, *in* THE FREE SPEECH CENTURY 254 (Lee C. Bollinger & Geoffrey R. Stone eds., 2018). On the end of the "utopian" phase, in which social media was often conceived of as a democratizing power for good, and the perils of growing platform power, see, for example, REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (2012); Jonathan Zittrain, Three Eras of Digital Governance (Oct. 7, 2019) (unpublished manuscript) (SSRN: https://perma.cc/TJN4-7TTX); *see also* Klonick, *The New Governors, supra* note 18; Evelyn Douek, *Governing Online Speech: From 'Posts-as-Trumps' to Proportionality and Probability*, 121 COLUM. L. REV. 754 (2021) (describing the evolution of platforms' content moderation policies from a deferential stance to balancing competing social interests).

[50] In the United States, public outrage and a slew of congressional hearings produced little by way of actual legal reform when it comes to the geopolitical and security aspects of platform operations. But as scholars have documented, informal pressure and fear of adverse regulatory action against private actors can be a powerful incentive for action. One could argue that platforms were partly "jawboned" into action by informal congressional and government pressure. *See, e.g.*, Derek E. Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51 (2015).

[51] On the latter, see Yoel Roth & Nick Pickels, *Updating Our Approach to Misleading Information*, TWITTER BLOG (May 11, 2020), https://perma.cc/7Y4C-MPNJ; Twitter Safety,

In other words, platforms have transitioned to proactivity *beyond* the platform. They replaced a relatively passive approach to what users posted with one that not only seeks to more aggressively moderate content on the platform, but also to monitor and identify threats in advance on an ongoing basis both online and, crucially, offline. In addition, platforms have recognized that a universal, "one content policy fits all" approach would no longer do. Local culture, sensitivities, and political context, they realized, must be accounted for in designing and implementing their policies.[52]

To that end, major platforms have created or significantly expanded dedicated teams and procedures to support what they call "trust and safety" or "integrity" operations. They have invested in building local expertise. They have developed a universe of related jargon and tradecraft. A steady pipeline of former national security and foreign policy government officials transitioned to platforms and transplanted government methods and modes of thinking into their growing trust and safety and public policy teams.

Since platforms lacked institutional capacity and expertise to independently contend with such a vast spectrum of geopolitical and security problems, platforms have also developed relationships with outside stakeholders to draw on their expertise, seek guidance, and benefit from intelligence to compensate for their blind spots when it comes to the offline world.

What follows briefly surveys internal organizational changes within three major platforms: Facebook, Google, and Twitter. Although similar developments have occurred in other companies,[53] I focus on those three platforms because of their role in recent security and geopolitical crises and the relative wealth of publicly available information about their trust and safety practices.[54] Part III then turns to external cooperation and the platform-government nexus.

COVID-19: Our Approach to Misleading Vaccine Information, TWITTER BLOG (Dec. 16, 2020), https://perma.cc/36YY-NH4A; Kang-Xing Jin, *Keeping People Safe and Informed About the Coronavirus*, FACEBOOK NEWSROOM (Dec. 18, 2020), https://perma.cc/4RL3-3LD7; Sundar Pichai, *COVID-19: How We're Continuing to Help*, GOOGLE KEYWORD (Mar. 15, 2020), https://perma.cc/N98G-V3RH.

[52] *See infra* Part II.B.

[53] *See* sources cited *supr*a note 3; *see also* Vanessa Pappas, *Combating Misinformation and Election Interference on TikTok*, TIKTOK (Aug. 5, 2020), https://perma.cc/C6U3-C3XS.

[54] The analysis could be applicable to other digital products and services that fall under the broad category of "platform." *See, e.g.*, Orly Lobel, *The Law of the Platform*, 101 MINN. L. REV.

B. Intra-Platform Capacity Building

Facebook, Google, and Twitter have all increased the number of employees with security and geopolitical responsibilities in the last few years. Former government national security policy experts and intelligence officers transitioning to the private sector assumed many of these new positions.[55] Facebook appears to have made the greatest and most publicized organizational adjustments. But all three companies have created or significantly expanded teams whose main task is to address geopolitical and security threats. They began to communicate related developments through periodic policy publications, data releases, and blog posts.

1. Facebook

Nothing exemplifies Facebook's geopolitical turn better than the docket of the newly established Facebook Oversight Board (FOB), Facebook's semi-independent organ for reviewing certain content moderation decisions.[56] Most of the cases that have reached the FOB's docket to date—covering a miniscule portion of Facebook's content decisions—touch on major geopolitical conflicts or security challenges. The cases implicate Alexei Navalny's opposition movement in Russia,[57] tensions in Turkey over the Armenian Genocide,[58] the conflict between Turkey and the Kurdistan Workers' Party (PKK),[59] the situation

87, 94-104 (2016). However, it primarily envisions dominant platforms that host or navigate access to user-generated content. Platforms that mostly facilitate transactions or access to services (Uber, TaskRabbit, Venmo) or host entertainment libraries (Netflix, Spotify) have not been central players in the national security and geopolitical space to date.

[55] *See, e.g.*, Victoria Kwan, *Facebook's Ex-Security Chief on Disinformation Campaigns: 'The Sexiest Explanation is Usually Not True'*, FIRST DRAFT (July 9, 2019), https://perma.cc/R9HE-SQ72 ("A lot of the people who work in the intelligence teams in companies like Google and Facebook come from Western intelligence agencies: the NSA, CIA, GCHQ and the like.").

[56] *See* Klonick, *The Facebook Oversight Board*, *supra* note 18; Douek, *supra* note 18.

[57] FACEBOOK OVERSIGHT BOARD, CASE DECISION 2021-004-FB-UA (2021) (Navalny Protests), https://perma.cc/QB5J-NS9J.

[58] FACEBOOK OVERSIGHT BOARD, CASE DECISION 2021-005-FB-UA (2021) (Armenian Hate Speech), https://perma.cc/H67J-UJVT.

[59] FACEBOOK OVERSIGHT BOARD, 2021-006-IG-UA USER APPEAL TO RESTORE CONTENT TO INSTAGRAM (2021) (requesting public comments in matter of PKK Founder Abdullah Öcalan), https://perma.cc/6KYP-DNS6.

in Myanmar,[60] the Israeli-Palestinian conflict,[61] protests in Colombia,[62] the Indian government's relationship with the country's Sikh population,[63] and the suspension of former President Donald Trump for inciting violence.[64]

Since 2016, Facebook has tripled the number of people working on trust and safety issues for the company. As of August 2021, they numbered around 40,000 in total.[65] Facebook's appointments to senior management roles reflect the company's effort to recalibrate its organizational infrastructure and procedures to generate better geopolitical analysis, monitor global threats, improve response protocols, and deepen ties with government around these activities. For example, in 2019, Facebook tapped Jennifer Newstead, the then-U.S. State Department Legal Adviser, for the position of General Counsel.[66] The appointment, among many others, signaled that the skill set Facebook seeks in its top legal officer is the skill set of the legal adviser to one of the world's foremost foreign policy and national security agencies.

The company has also created or reframed dedicated positions to bring centralized, high-level attention to geopolitical and security threats. This includes the positions of Head of Cybersecurity Policy, currently held by a former Director for Cybersecurity Policy at the National Security Council

---

[60] FACEBOOK OVERSIGHT BOARD, CASE NUMBER AND SUMMARY 2021-007-FB-UA (2021) (requesting public comments in matter of situation in Myanmar and profanity on the platform), https://perma.cc/F9U8-8T9P.

[61] FACEBOOK OVERSIGHT BOARD, 2021-009-FB-UA USER APPEAL TO RESTORE CONTENT TO FACEBOOK (2021) (requesting public comments in matter of Al Jazeera Post on Israel-Palestine), https://perma.cc/ZJX2-JT5T.

[62] FACEBOOK OVERSIGHT BOARD, 2021-010-FB-UA USER APPEAL TO RESTORE CONTENT TO FACEBOOK (2021) (requesting public comments in matter of protests in Colombia), https://perma.cc/8ED5-6DAH.

[63] FACEBOOK OVERSIGHT BOARD, CASE DECISION 2021-003-FB-UA (2021) (Modi and Indian Sikhs), https://perma.cc/Z9WR-2NUS.

[64] FACEBOOK OVERSIGHT BOARD, CASE DECISION 2021-001-FB-FBR (2021) (Trump Suspension), https://perma.cc/LU6D-CQRP.

[65] *See* Clegg, *supra* note 43; *Our Progress Addressing Challenges and Innovating Responsibly*, META NEWSROOM (Sept. 21, 2021), https://perma.cc/9NEJ-BTMP; *see also* Joshua Fruhlinger, *Facebook Ramps Up Hiring for "Privacy", "Security", and "Trust" Related Jobs*, B[2] THE BUSINESS OF BUSINESS (May 2, 2019), https://perma.cc/4H7X-PMUD ("Keyword trends reveal that Facebook went on a hiring spree for professionals skilled in security and information safety as the brand looks to rebuild trust with users. In fact, job titles with the words 'security, safety, privacy, or trust' are now five times higher than they were just a couple years ago, and 37% higher than the summer of 2018.").

[66] *Jennifer Newstead to Join Facebook as General Counsel and John Pinette Becomes Vice President of Global Communications*, FACEBOOK NEWSROOM (Apr. 22, 2019), https://perma.cc/B7CY-FR76.

(NSC),[67] and the position of Global Threat Disruption Lead within Facebook's Public Policy unit, currently held by a former NSC Director of Intelligence.[68] Job postings for Facebook positions such as "Law Enforcement Signal Intelligence Specialist" state:

> Teams across Facebook are dedicated to preventing real world harm and countering threats, often working with governments around the world . . . . Our Strategic Initiatives team, which coordinates efforts across our law enforcement-related programs, is looking for a Law Enforcement Signal Intelligence Specialist to identify insights . . . and drive strategy to enable the company to anticipate and leverage emerging trends. The position will help us to gain a deeper understanding of how bad actors use Facebook, analyze current safety trends, and develop solutions to detect and mitigate risk.[69]

It is not entirely clear to the outside observer how Facebook's vast safety and security apparatus is organized internally, but some details have been shared with the public or revealed by researchers.[70]

i. Counterterrorism and Violent Extremism

To start, Facebook significantly ramped up organizational capacity in the areas of terrorism and countering violent extremism. Facebook—at its inception, a social network used for mundane purposes such as keeping up with friends and sharing photos—now employs a Counterterrorism Policy and Dangerous Organizations Manager.[71] In late 2017, the company had more than 4,500 content reviewers working in "community operations teams" around the

---

[67] *Nathaniel J. Gleicher Biography*, CTR. FOR STRATEGIC & INT'L STUD., https://perma.cc/M29N-A43T.

[68] *See* David Agranovich, Global Threat Disruption Lead, Facebook, Brookings Institution Webinar: Election Integrity and Security in the Era of COVID-19, at 1 (July 17, 2020), https://perma.cc/4WHN-PV24 [hereinafter Brookings Panel].

[69] Facebook, *Law Enforcement Signal Intelligence Specialist Job*, LENSA, https://perma.cc/2BNW-2FUR.

[70] Kate Klonick's work on Facebook content moderation and the Facebook Oversight Board, for instance, includes detailed, first-hand accounts of certain aspects of this apparatus. *See, e.g.*, Klonick, *The New Governors*, *supra* note 18; Klonick, *The Facebook Oversight Board*, *supra* note 18.

[71] Paul Cruickshank, *A View from the CT Foxhole: An Interview with Brian Fishman, Counterterrorism Policy Manager, Facebook*, CTC SENTINEL, Sept. 2017, at 8.

world to address terrorist content, among other forms of potentially harmful content. [72] By 2018, that number had increased to 7,500 moderators.[73]

In addition to "line" content moderators, Facebook has created a team of counterterrorism specialists whose responsibility is to help develop policy and review the determinations of content moderators in hard cases. That team consists of about 150 specialists with backgrounds in academia, prosecution, law enforcement, and engineering.[74] According to Facebook, team members are proficient in nearly thirty languages to account for local context.[75]

Furthermore, Facebook has said that it works with external partners to get intelligence and develop insights about threat actor behavior offline and that it leverages "off-platform signals" to identify dangerous content. Facebook has asserted that these efforts have significantly increased proactive detection of organized hate—that is, the percentage of content Facebook removes on its

---

[72] Facebook executives have highlighted the importance of human review in light of existing artificial intelligence technology's limitations in judging content in context, particularly in areas such as terrorism, violent extremist propaganda, and hate speech. *See* Alexis C. Madrigal, *Inside Facebook's Fast-Growing Content-Moderation Effort*, ATLANTIC (Feb. 7, 2018), https://perma.cc/K42R-58FU; Cruickshank, *supra* note 71, at 8-9 ("Context is everything, so we really need human beings to help us understand and make those decisions.").

[73] Cruickshank, *supra* note 71, at 8, 11; Madrigal, *supra* note 72 (reporting that Facebook's VP of Global Policy "emphasized that humans are deeply necessary to the project of content moderation, saying that Facebook now has 7,500 content moderators around the world, meeting the hiring goal Mark Zuckerberg set in May of 2017 . . . . In other words, they've added almost the same number of content moderators as Twitter or Snapchat's total employee head count in the last eight months"). On the work of content moderators, see generally SARAH T. ROBERTS, BEHIND THE SCREEN: CONTENT MODERATION IN THE SHADOWS OF SOCIAL MEDIA (2019); *see also* Klonick, *The New Governors*, *supra* note 18; Kate Klonick, *Inside the Team at Facebook That Dealt with the Christchurch Shooting,* NEW YORKER (Apr. 25, 2019), https://perma.cc/Q9YU-BERF; Casey Newton, *The Trauma Floor: The Secret Lives of Facebook Moderators in America*, VERGE (Feb. 25, 2019), https://perma.cc/JRR6-6P9S.

[74] Monika Bickert & Brian Fishman, *Hard Questions: How We Counter Terrorism*, FACEBOOK NEWSROOM (June 15, 2017), https://perma.cc/A6BL-4ZDG; Monica Bickert & Brian Fishman, *Hard Questions: What Are We Doing to Stay Ahead of Terrorists*, FACEBOOK NEWSROOM (Nov. 8, 2018), https://perma.cc/4MWA-M8RT.

[75] Cruickshank, *supra* note 71, at 9. Facebook's Head of Counterterrorism Policy has addressed the importance of localized expertise in his area: "I think that the biggest point of learning for me is figuring out how to scale an operation to enforce guidelines consistently and effectively. And in my experience, until you've had to manage the scale that Facebook operates at, even when somebody gives you some of the numbers, you still have to learn to wrap your head around it and understand what that means in terms of language coverage, cultural knowledge, having the right people to be able to do the right things." *Id.* at 8, 11.

own initiative, before users report it.[76] According to Facebook's community standards enforcement report for the first quarter of 2021, the "proactive rate" for content it enforced against based on its dangerous organizations policy was 99.6%.[77]

Facebook has also increased enforcement against domestic terrorism and violent extremism, especially in the wake of the 2020 U.S. election and the January 6, 2021 Capitol riots. It did so despite internal pushback due to concern over political blowback.[78] Facebook removed tens of thousands of accounts, pages, and groups belonging to militarized groups such as the Proud Boys, as well as "violence-inducing conspiracy networks" like QAnon.[79] At the time, the company said it had identified "over 890 militarized social movements to date."[80]

ii. Election Integrity and Influence Operations

Similar developments occurred in policy areas other than counterterrorism and violent extremism. Since 2016, Facebook significantly ramped up its efforts to "stop information operations, including those that target elections."[81] Those efforts have a strong geopolitical tilt because they emphasize state-backed influence operations. "Foreign-led efforts to manipulate public debate in another country" and "[o]perations run by a government to target its own

---

[76] *An Update on Combating Hate and Dangerous Organizations*, FACEBOOK NEWSROOM (updated May 14, 2020), https://perma.cc/MU2M-N3VM [hereinafter: *2020 Dangerous Orgs Update*]; *see also* Brian Fishman, *Crossroads: Counter-Terrorism and the Internet*, 2 TEX. NAT'L SEC. REV. 83, 83 (2019) ("[I]n the first nine months of 2018, Facebook removed 14.3 million pieces of content related to the Islamic State, al-Qaeda, and their affiliates, only 41,000 of which were flagged by external sources, primarily regular users. The overwhelming majority of the content removed came as a result of Facebook's voluntary internal efforts.").

[77] *Dangerous Organizations: Terrorism and Organized Hate*, FACEBOOK TRANSPARENCY CTR., https://perma.cc/ZRP3-WSN8.

[78] *See* Ryan Mac & Craig Silverman, *"Mark Changed the Rules": How Facebook Went Easy on Alex Jones and Other Right-Wing Figures*, BUZZFEED NEWS (Feb. 22, 2021), https://perma.cc/H5UG-8ZWC.

[79] *See* Rosen & Bickert, *supra* note 3; *An Update to How We Address Movements and Organizations Tied to Violence*, FACEBOOK NEWSROOM (updated Jan. 19, 2021), https://perma.cc/XAE3-B2RD.

[80] *Id.*

[81] Nathaniel Gleicher, *How Do We Work With Our Partners to Combat Information Operations?*, FACEBOOK NEWSROOM (Nov. 13, 2018), https://perma.cc/LD23-5WZ9; Guy Rosen, Katie Harbath, & Nathaniel Gleicher, *Helping to Protect the 2020 US Elections*, FACEBOOK NEWSROOM (Oct. 21, 2019), https://perma.cc/BXM5-YS25.

citizens," according to Facebook, are "particularly egregious" forms of deception on the platform.[82]

Facebook's cybersecurity, threat disruption, and global elections teams tasked with these responsibilities include members with "backgrounds in cybersecurity, digital forensics, national security, foreign policy and law enforcement." [83] The teams collaborate with governments and other stakeholders worldwide to "proactively monitor" threats.[84] They engage in "deep investigations on platforms" to uncover "coordinated inauthentic behavior"—an ill-defined term Facebook coined. [85] They synthesize technological insights about threat actor methods and other information gleaned from the platform with information about offline behavior and relationships available to the government and other players.[86] Insights about threat actor behavior in turn inform the development of technology for automated defense at scale against similar threats.[87] Recently, Facebook began to target *authentic* accounts that coordinate social harm on the platform—not just fake accounts and diversion designed to conceal who is behind harmful operations.[88]

A central element of this evolving policy and practice has been turning the focus to online and offline user conduct, as distinct from moderating pieces of content as they are posted on the platform.[89] The focus on behavior inherently

---

[82] Nathaniel Gleicher, *How We Respond to Inauthentic Behavior on Our Platforms: Policy Update*, FACEBOOK NEWSROOM (Oct. 21, 2019), https://perma.cc/UU7G-7KCF.

[83] Gleicher, *supra* note 81; *see also How Facebook Has Prepared for the 2019 UK General Election*, FACEBOOK NEWSROOM (Nov. 7, 2019), https://perma.cc/ZU6T-SAS4 (featuring remarks by Nathaniel Gleicher).

[84] Gleicher, *supra* note 81.

[85] Brookings Panel, *supra* note 68, at 48.

[86] Gleicher, *supra* note 81; Brookings Panel, *supra* note 68, at 43, 46-48 (David Agranovich: "My team focuses on both the coordination of our investigations and disruptions of [information operations aimed at election interference] on Facebook, as well as thinking through some of the scenario planning around what new tactics do we anticipate seeing as these operations evolve and adapt to the enforcement that's being taken against them on different platforms.").

[87] *How Facebook Has Prepared for the 2019 UK General Election*, *supra* note 83 ("For each investigation, we isolate any new behaviors we see and then we work to automate detection . . . at scale.").

[88] Nathaniel Gleicher, *Removing New Types of Harmful Networks*, FACEBOOK NEWSROOM (Sept. 16, 2021), https://perma.cc/4Q3W-5HCJ.

[89] *See* Brookings Panel, *supra* note 68, at 46. Facebook's heads of cybersecurity policy and global threat disruption have explained that the focus on behavior neutralizes the

involves proactive research and analysis reminiscent of traditional government intelligence analysis work.[90] For instance, Facebook must identify the interests and geopolitical objectives of Russia and be familiar with the actors spreading disinformation on its behalf to prepare for a U.S. election. It must understand Iran's global and regional posture to counter influence operations backed by Tehran.

Proactive monitoring and analysis of coordinated inauthentic behavior on Facebook's platforms have produced multiple takedowns of networks and content in the last few years. Facebook boasted a 99.8% "proactive rate" on fake accounts for the first quarter of 2021.[91] The company advertises these takedowns as they take place or in cumulative monthly reports, which it started issuing in early 2020.[92] The first network Facebook took down in 2017 was linked to the Russian Internet Research Agency (IRA) and its effort to influence the 2016 U.S. election.[93] In late 2019, Facebook reported that it had removed

---

significance of other tricky parameters such as the nature of the content posted (which does not always technically violate platform terms of service), the identity of the actor as foreign or domestic (which could trigger complex questions about action against U.S.-based networks operating for political goals), and whether the actions of those engaged in coordinated inauthentic behavior can be attributed to a state actor like China or Russia (which is often difficult to prove). *See* Alex Stamos, *How Does Facebook Investigate Cyber Threats and Information Operations?*, FACEBOOK NEWSROOM (Nov. 14, 2018), https://perma.cc/43GE-G5TJ; Kristen Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520 (2020). This approach has been criticized, primarily on grounds that Facebook has failed to clearly define and explain what constitutes "coordinated inauthentic behavior" that could result in heightened transparency requirements, content removal, or wholesale deplatforming. *See* Evelyn Douek, *What Does "Coordinated Inauthentic Behavior" Actually Mean?*, ATLANTIC (July 2, 2020), https://perma.cc/S72K-8NEH.

[90] *See* Katie Harbath & Samidh Chakrabarti, *Expanding Our Efforts to Protect Elections in 2019*, FACEBOOK NEWSROOM (Jan. 28, 2019), https://perma.cc/22GV-6G8H ("Over the past two years, we have made massive investments to help protect the integrity of elections—not only addressing threats we've seen on our platform in the past, but also anticipating new challenges and responding to new risks. . . . While these efforts are global, we also customize our work to individual countries based on research and threat assessments that begin many months before ballots are cast.").

[91] *Fake Accounts*, FACEBOOK TRANSPARENCY CTR., https://perma.cc/U4HX-JK39.

[92] *See, e.g.*, *December 2020 Coordinated Inauthentic Behavior Report*, FACEBOOK NEWSROOM (Jan. 12, 2021), https://perma.cc/P7AU-YXAF (describing takedown of 17 influence operations on nearly every continent); *August 2020 Coordinated Inauthentic Behavior Report*, FACEBOOK NEWSROOM (Sept. 1, 2020), https://perma.cc/K26S-EDRA; *February 2020 Coordinated Inauthentic Behavior Report*, FACEBOOK NEWSROOM (Mar. 2, 2020), https://perma.cc/8MTR-SV7X.

[93] Alex Stamos, *Authenticity Matters: The IRA Has No Place on Facebook*, FACEBOOK NEWSROOM (Apr. 3, 2018), https://perma.cc/Z4P8-PCWS. *Compare id.*, *with Update on Twitter's Review*

fifty networks engaged in coordinated inauthentic behavior worldwide the previous year, many ahead of major elections.[94] That number doubled to one hundred by August 2020,[95] with around ten additional takedowns announced each month since.[96]

These efforts have proved somewhat successful in preventing foreign election interference. In the aftermath of the 2020 U.S. election, Facebook reported that there were few successful attempts by foreign actors to spread disinformation, and that the small number of operations that were detected did not gain much traction. Facebook attributed this to platforms making it difficult for foreign-backed networks to use methods deployed in 2016. Instead, a key challenge became what Facebook officials have called "perception hacking"—efforts by various actors to create the impression that foreign

---

of the 2016 US Election, TWITTER BLOG (Jan. 19, 2018), https://perma.cc/6J99-37KY (discussing suspension of thousands of IRA accounts), and Taylor Hatmaker, *Google Offers New Findings on Russian Disinformation Across its Products*, TECHCRUNCH (Oct. 30, 2017), https://perma.cc/32PS-JHAQ.

[94] Rosen et al. *supra* note 81 .

[95] FACEBOOK, DETAILED REPORT: AUGUST 2020 COORDINATED INAUTHENTIC BEHAVIOR REPORT 3, (2020) ("Since 2017, we have removed over 100 networks worldwide for engaging in coordinated inauthentic behavior, including ahead of major democratic elections. The first network we took down was linked to the Russian Internet Research Agency (IRA), and so was the 100th we removed in August.").

[96] *Coordinated Inauthentic Behavior*, FACEBOOK, https://perma.cc/37VM-RZ6P. For example, in 2019, the company announced the removal of four networks that originated in Iran and Russia and targeted the U.S., North Africa and Latin America. Facebook explained that it had "identified these manipulation campaigns as part of [its] internal investigations into suspected Iran-linked inauthentic behavior, as well as ongoing proactive work ahead of the US elections." Rosen, et al., *supra* note 81. The company underscored that the removal decision was based on the networks' deceptive practices, not the content that it posted, and that it had shared its findings with law enforcement and industry partners. Facebook added that the action required its teams to build "a deeper understanding of different threats and how best to counter them". *See id.*

In March 2020, Facebook announced that it had removed hundreds of accounts and dozens of pages for engaging in coordinated inauthentic behavior on behalf of Russia. The network attempted to conceal its operations by working through Nigerian and Ghanaian nationals. It primarily targeted the United States. Facebook again said that the takedown was a product of its internal investigation into suspected coordinated inauthentic behavior ahead of the U.S. election, and highlighted cooperation with policymakers, law enforcement, industry peers and investigative journalists. Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior from Russia*, FACEBOOK NEWSROOM (Mar. 12, 2020), https://perma.cc/QC8H-4RG2.

influence was much more significant than it was, undermining voters' faith in the validity of the election outcome.[97]

U.S. elections have not been Facebook's only focus. In 2018, the company launched a global Election Operations Center employing intelligence and policy experts.[98] Recently, it floated the idea of establishing an Election Commission to advise on related decisions.[99] Facebook has issued updates about its preparation for elections in a variety of countries. For example, ahead of the 2019 United Kingdom general election, Facebook's head of U.K. public policy announced the formation of an Elections Taskforce with national, regional, and headquarter representation to work on, among other things, threat intelligence. The task force was touted as a war room of sorts to complement the other ongoing security efforts described above.[100] Facebook took similar steps ahead of elections in Indonesia,[101] Australia,[102] Thailand,[103] and India,[104] among others.[105]

---

[97] *See* FACEBOOK, A LOOK AT FACEBOOK AND U.S. 2020 ELECTIONS 5-6 (2020), https://perma.cc/69QL-YBNL [hereinafter FACEBOOK 2020 REPORT]; *see also* Nathaniel Gleicher, Head of Cybersecurity Pol'y, Facebook, remarks at the Stanford Freeman Spogli Institute Cyber Policy Center conference: Digital Technology, Social Media and the 2020 Presidential Election (Dec. 10, 2020) (transcript on file with the author) [hereinafter Stanford 2020 Election Panel].

[98] FACEBOOK 2020 REPORT, *supra* note 97, at 8; *see also* Guy Rosen, *Preparing for Election Day*, FACEBOOK NEWSROOM (Oct. 7, 2020), https://perma.cc/55L5-UWRX.

[99] *See* Ryan Mac, Mike Isaac & Sheera Frenkel, *Facebook Said to Consider Forming an Election Commission*, N.Y. TIMES (Aug. 25, 2021), https://perma.cc/834C-3Z8R.

[100] *How Facebook Has Prepared for the 2019 UK General Election*, *supra* note 83.

[101] Katie Harbath & Ruben Hattari, *Working to Safeguard Elections in Indonesia*, FACEBOOK NEWSROOM (Mar. 4, 2019), https://perma.cc/FR2D-6R4U.

[102] Mia Garlick, *Working to Safeguard Elections in Australia*, FACEBOOK NEWSROOM (Apr. 4, 2019), https://perma.cc/P22C-GPGH.

[103] Katie Harbath & Roy Tan, *Working to Safeguard Elections in Thailand*, FACEBOOK NEWSROOM (Jan. 30, 2019), https://perma.cc/FXG8-58J4.

[104] *Our Steps to Protect State Elections in India*, FACEBOOK NEWSROOM (Mar. 30, 2021), https://perma.cc/QBP2-3DSM; Ajit Mohan, *Preparing for Upcoming Indian Elections,* FACEBOOK NEWSROOM (Apr. 8, 2019), https://perma.cc/RHL9-7PFX.

[105] The policy updates ahead of each round of elections were issued by Menlo Park leadership, local and regional public policy heads, or (often) some combination of headquarters and local officials. The participation of local policy officials exemplifies the role of localized expertise in Facebook's election integrity policy, similar in some ways to the role that embassies and country intelligence play in formulating traditional foreign and security policy.

iii. Global Conflicts

Facebook has ostensibly taken steps to avoid repeating what took place in global hotspots like Myanmar and Thailand. The company was slow to respond to the spread of propaganda and incitement on its platforms in those conflict areas, contributing to large-scale sectarian and religious violence. In Myanmar, many blamed Facebook for contributing to mass atrocities against the Rohingya minority.[106] Consequently, Facebook created a Strategic Response team to tackle escalation to violence in conflict areas.[107] The team has been described as the "latest evolution in the Silicon Valley's culture: less 'move fast and break things,'[108] and more thinking through the harm they are adding to half a world away."[109]

Like the other Facebook security and geopolitics teams discussed here, the Strategic Response team consists of individuals with experience in government, military, and geopolitical risk assessment in large multinational corporations.[110] The team is designed to fill a coordination gap among Facebook's various units in responding to global conflicts. It reports directly to Facebook's senior leadership. Its tasks include recommending technological product adjustments to make it more difficult for disinformation and propaganda to spread in conflict areas, coordinating the platform's response where there are indications on the ground that a crisis could be imminent, and advising the company on capacity building for these tasks.[111]

Recent Facebook actions attempted to implement some of the lessons learned from past conflicts. In the wake of the February 2021 military coup in

---

[106] *See* sources cited *supra* notes 5-6.

[107] *See* Ingram, *supra* notes 7-8.

[108] Facebook's now-infamous motto, which guided the company early on but was abandoned in 2014 in favor of "move fast with stable infrastructure." *See* LEVY, *supra* note 37, at 235-74.

[109] *See* Ingram, *supra* notes 7-8.

[110] *Id.* ("Software engineers have been the core of Silicon Valley companies like Facebook, but lately the office parks housing America's tech mega-corporations are seeing more people in key roles who used to work inside governments, the military or multinational corporations at risk of sparking violence in the world's hot spots.").

[111] *Id*. The team has been criticized for being too small to be effective and lacking sufficient presence on the ground in conflict regions to generate relevant expertise and policy options. Facebook has said that it relies extensively on local NGOs for local expertise and context, and that it dispatches staff on country visits. The team appears to have at least some regional presence. *Id.* For our purposes, however, the key is that the company is thinking about and retooling for addressing quintessential geopolitical challenges—sectarian and religious conflicts.

Myanmar, Facebook did not wait long before deplatforming the entire Myanmar military (Tatmadaw) and linked entities.[112] In a different context, Facebook dispatched its top global affairs and public policy executives to meet with Israeli and Palestinian officials during the May 2021 clash between Israel and Gaza and sectarian violence within Israel.[113] This was in response to criticism that Facebook was not doing enough to curb the spread of violence through its platforms. The platform also adopted the "war room" model from the election context. It formed a "special operations center" to monitor the situation and improve enforcement against disinformation, incitement to violence, and coordination of violence in real time.[114]

2. Twitter

Other major platforms have created similar intelligence analysis, policy, and outreach units, albeit on a smaller scale compared to Facebook. Twitter has similarly expanded its organizational infrastructure to better address security and geopolitical threats to its platform. Contending with geopolitical threats was not a task that Twitter had emphasized prior to 2016, as the company's acting General Counsel conceded in a 2017 testimony before a Senate Judiciary subcommittee.[115]

---

[112] Rafael Frankel, *An Update on the Situation in Myanmar*, FACEBOOK NEWSROOM (Feb. 11, 2021), https://perma.cc/U486-85SG. The coup took place on February 1, 2021. *Id.*

[113] Emily Birnbaum, *Facebook Meets with Israeli and Palestinian Officials to Discuss Online Hate Speech*, *Threats as Violence Escalates*, POLITICO (May 14, 2021), https://perma.cc/4RR5-J75Z.

[114] *See* Culliford, *supr*a note 12.

[115] *Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions Before the Subcomm. on Crime & Terrorism of the Sen. Comm. on the Judiciary*, 115th Cong. 1 (2017) (statement of Sean J. Edgett, Acting General Counsel, Twitter, Inc.,) https://perma.cc/8G8A-4MFR [hereinafter Edgett Testimony]. Speaking about foreign influence operations, Edgett described the "abuse of [the] platform by sophisticated foreign actors to attempt state-sponsored manipulation of elections" as a "new challenge" for Twitter—and "one that [Twitter is] determined to meet." He told the subcommittee that Twitter had created a dedicated team to block malicious activity on the platform in coordination with government and industry peers. *Id.* at 1-2; *see also* Carlos Monje Jr., *2018 US Midterm Elections Review*, TWITTER BLOG (Jan. 31, 2019), https://perma.cc/ZN3K-DPMR; Del Harvey & Yoel Roth, *An Update on Our Election Integrity Work*, TWITTER BLOG (Oct. 1, 2018), https://perma.cc/EWX3-W7R9.

Like Facebook, Twitter has emphasized the security and geopolitical challenges of terrorism and violent extremism,[116] election integrity, countering influence operations, and COVID-19[117] in its post-2016 efforts to protect the platform from abuse. Twitter's Safety and Site Integrity teams lead the company's efforts to identify and investigate suspected platform manipulation and other violations of Twitter's policies. The Twitter teams partner with governments, law enforcement, and industry peers to "improve our understanding of the actors involved in information operations and develop a holistic strategy for addressing them."[118] Those working on these issues within Twitter include "data scientists, linguists, policy analysts, political scientists, and technical experts."[119] The company has vowed to bring in additional personnel to support platform safety work.[120]

As part of the reforms introduced post-2016, Twitter has expanded its biannual transparency report—which originally focused on disclosure of information about government requests Twitter receives under various legal

---

[116] *See* Edgett Testimony, *supra* note 115, at 16-17; Twitter Public Policy, *Addressing the Abuse of Tech to Spread Terrorist and Extremist Content*, TWITTER BLOG (May 15, 2019), https://perma.cc/2UWM-PNFH. Twitter has acted aggressively against accounts on terrorism grounds at a relatively early stage. Between 2015-2017, the platform suspended 1.2 million accounts for terrorism links. *See* Don Reisinger, *Twitter Has Suspended 1.2 Million Terrorist Accounts Since 2015*, FORTUNE (Apr. 5, 2018), https://perma.cc/N46M-WQKW; Danny Yadron, *Twitter Deletes 125,000 ISIS Accounts and Expands Anti-Terror Teams*, GUARDIAN (Feb. 5, 2016), https://perma.cc/64HP-WTRQ. Twitter has also been active in addressing violent extremism, including by domestic actors in the U.S. It was a first mover on the deplatforming of accounts associated with the QAnon conspiracy. *See infra* note 146. The company also took action to stem violent extremism in other countries. *See, e.g.*, Twitter Safety, *Updates on Our Response to Blocking Orders from the Indian Government*, TWITTER BLOG (Feb. 10, 2021), https://perma.cc/72AV-FMZ2.

[117] *See* sources cited *supra* note 51.

[118] Yoel Roth, *Information Operations on Twitter: Principles, Process, and Disclosure*, TWITTER BLOG (June 13, 2019), https://perma.cc/WHR4-87L5; *see also* Vijaya Gadde & Yoel Roth, *Enabling Further Research of Information Operations on Twitter*, TWITTER BLOG (Oct. 17, 2018), https://perma.cc/B4PC-HEZN ("information operations and coordinated inauthentic behavior will not cease. These types of tactics . . . will adapt and change as the geopolitical terrain evolves worldwide and as new technologies emerge. . . . [W]e are committed to understanding how bad-faith actors use our services. We will continue to proactively combat nefarious attempts to undermine the integrity of Twitter, while partnering with civil society, government, our industry peers, and researchers to improve our collective understanding of coordinated attempts to interfere in the public conversation. Our dedicated site integrity team, in partnership with a diverse range of committed organizations and personnel across the company, continue to invest heavily in this area.")

[119] Roth, *supra* note 118.

[120] Monje, *supra* note 115.

authorities—to include sections on the enforcement of the Twitter Rules.[121] The reports show that like Facebook, Twitter engages in proactive enforcement against terrorism and violent extremism, which requires independent monitoring and intelligence. For example, between July and December 2020 alone, Twitter enforced against 58,750 unique accounts under this policy. The company asserted that 96% of those actions were taken on the platform's own initiative without first being reported by users.[122]

Election integrity has been another key security challenge that Twitter has prioritized. Around the 2020 U.S. election, the company took steps to limit the spread of disinformation and incitement to violence under a combination of policies, including policies on civic integrity and against glorification of violence and coordinated harmful activity.[123] For instance, following the January 6 Capitol riots, Twitter suspended upward of 70,000 QAnon-associated accounts.[124] The company also famously suspended President Trump.[125]

Like their Facebook counterparts, the Twitter site integrity team's information operations work focuses on enforcement against coordinated and deceptive behavior. Twitter's public disclosure policy with respect to such behavior focuses on activity verifiably attributable to state actors.[126] The company now maintains a public archive of tweets and media connected to state-backed information operations.[127] The dataset includes accounts linked to China, Russia, Saudi Arabia, Ghana, Nigeria, Iran and several other countries.[128] To date, Twitter has disclosed over 85,000 accounts linked to state-backed information operations.[129]

Twitter has said that disclosure of state-sponsored manipulation of the platform is in the public interest because "people and organizations with the advantages of institutional power and which consciously abuse our service are

---

[121] Twitter Public Policy, *Evolving our Twitter Transparency Report: Expanded Data and Insights*, TWITTER BLOG (Dec. 12, 2018), https://perma.cc/7A22-MX26.

[122] *See Rules Enforcement Report, July-December 2020*, TWITTER TRANSPARENCY, https://perma.cc/7E6H-NLPS.

[123] Twitter Safety, *Expanding Our Policies to Further Protect the Civic Conversation*, TWITTER BLOG (Sept. 10, 2020), https://perma.cc/SHL6-R39Z.

[124] Twitter Safety, *An Update Following the Riots in Washington DC*, TWITTER BLOG (Jan 12, 2021), https://perma.cc/ZVV2-ZDGB.

[125] Twitter Inc., *supra* note 3.

[126] Roth, *supra* note 118.

[127] *Information Operations*, TWITTER TRANSPARENCY REPORT, https://perma.cc/3HNN-U8ZT.

[128] *Id.*

[129] *Id.*

not advancing healthy discourse but are actively working to undermine it."[130] Much like Facebook's framing of state-sponsored coordinated activity as a particularly "egregious" threat,[131] Twitter's emphasis on state actors in its disclosure policy highlights the geopolitical nature of these efforts.

3. Google

Google and its parent, Alphabet, have arguably been the least transparent and forthcoming about their internal efforts to tackle threats to the company's various products. Still, what we do know about Google's current posture indicates that it has engaged in similar institutional capacity building in the areas of security and management of geopolitical threats.

Most notably, Google formed a Threat Analysis Group (TAG) to counter government-backed attacks across its platforms, including YouTube.[132] TAG's current head is a former Australian intelligence official, and it has been described as a "small intelligence agency" and "one of the nation's massive private counterespionage efforts."[133] The group began producing public updates about its work in August 2018, covering issues such as state-sponsored activity, the maintenance of platform integrity, the protection of users from government-backed hacking and disinformation, and COVID-19.[134]

Like Facebook and Twitter, Google has highlighted its efforts to counter "coordinated influence operations" both online and offline through cooperation with other stakeholders, among other measures.[135] For instance, in 2019, TAG announced that Google acted against Russia-affiliated influence

---

[130] Roth, *supra* note 118.

[131] Gleicher, *supra* note 82.

[132] *See* Shane Huntley, *Maintaining the Integrity of Our Platforms*, KEYWORD (Aug. 22, 2019), https://perma.cc/FXM9-KSFT.

[133] Robert McMillan, *Inside Google's Team Fighting to Keep Your Data Safe from Hackers*, WALL ST. J. (Jan. 23, 2019), https://perma.cc/ALY2-ASX3.

[134] *Threat Analysis Group: The Latest on Our Efforts to Counter Government-Based Attacks*, GOOGLE OFFICIAL BLOG, https://perma.cc/2DKC-QBSF.

[135] Shane Huntley, *Updates about Government-Backed Hacking and Disinformation*, GOOGLE: UPDATES FROM THE THREAT ANALYSIS GROUP (May 27, 2020), https://perma.cc/SH6K-9SDG ("On any given day, Google's Threat Analysis Group (TAG) is tracking more than 270 targeted or government-backed attacker groups from more than 50 countries."); Huntley, *supra* note 132; Shane Huntley, *Protecting Users from Government-Backed Hacking and Disinformation*, GOOGLE THREAT ANALYSIS GROUP (Nov. 26, 2019), https://perma.cc/7CVE-UA8V [hereinafter Huntley, *Protecting Users*].

operations targeting several nations in Africa.[136] The company noted that this move was consistent with similar Facebook action. The operations involved use of inauthentic news outlets to promote Russian interests.[137]

In early 2020, Google's head of Trust and Safety outlined the company's efforts to combat election interference ahead of the 2020 U.S. election:

> As part of our ongoing efforts to counter interference on our platforms, we work closely with other technology companies and government agencies, such as the FBI's Foreign Influence Task Force, on referrals and leads. Alongside my colleagues at Google's Threat Analysis Group, and at YouTube, we work closely to identify bad actors, disable their accounts, warn our users about them, and share relevant information with industry officials and law enforcement.[138]

Google has harnessed Alphabet's in-house think tank and technology incubator, Jigsaw, to support this work. Jigsaw's mission is to "identify emerging issues . . . that threaten open society" and to build technology to address significant security challenges.[139] Two of its four main areas of work are disinformation and violent extremism.[140] Jigsaw research supported Google's investigation into foreign interference in the 2016 U.S. elections.[141]

Finally, Google created new intelligence synthesis and risk assessment roles such as a "Trust and Safety Lead for Intelligence and Insight" and a "Strategic Intelligence Manager for Emerging Trends and Risk Management."[142] The

---

[136] Huntley, *Protecting Users*, *supra* note 135.

[137] *Id*.

[138] Kristie Canegallo, *Supporting the 2020 U.S. Election*, KEYWORD (Feb. 3, 2020), https://perma.cc/BV2M-TQG9; *see also Foreign Influence Operations' Use of Social Media Platforms: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 2 (2018) (written testimony of Kent Walker, Senior Vice President, Global Affairs & Chief Legal Officer, Google) ("Google remains deeply concerned about attempts to undermine democratic elections.").

[139] *Approach: Confronting Threats to Open Societies with Scalable Solutions*, JIGSAW, https://perma.cc/QWY9-WQ45.

[140] *A Safer Internet Means a Safer World*, JIGSAW, https://perma.cc/7FK8-6PCQ (describing Jigsaw as a unit within Google that "forecast[s] emerging threats and explore[s] how technology can protect individuals and societies").

[141] Walker, *supra* note 138, at 1.

[142] William McCants, LINKEDIN, https://perma.cc/7QZQ-DSFU; Tobias Peyerl, LINKEDIN, https://perma.cc/FWC3-32MR.

company hired counter-terrorism specialists and other subject-matter experts.[143]

III. THE PLATFORM-GOVERNMENT NEXUS

The previous Part focused on platforms' internal efforts to build organizational capacity to meet a variety of security and geopolitical challenges affecting their products. This Part turns to the external aspects of these efforts. It considers the expansion of inter-platform cooperation and the broadening of the platform-government nexus in addressing key national and global security challenges facing governments and platforms alike. It also explores how platforms have replicated traditional government national security practices. The final section of this Part reflects on the role of existing law in enabling and facilitating these dynamics.

A. Direct Platform-Government Cooperation

The past few years have seen growing cooperation between platforms and other stakeholders to address global and national security challenges. Some of this cooperation focuses on ad hoc information sharing and responding to specific incidents, while other, long-term forms of cooperation are reminiscent of institutionalized inter-agency processes or traditional international organizations.

1. Incident-Centered Cooperation

It has become increasingly common for platforms to work together against specific actors and information operations. Platforms often announce the identification and removal of information operations simultaneously or in close proximity, reference other platforms' actions in announcing their own, or include boilerplate language in their takedown announcements to the effect

---

[143] Kristie Canegallo, *Meet the Teams Keeping Our Corner of the Internet Safer*, KEYWORD (Feb. 5, 2019), https://perma.cc/8XWF-FF28 ("Take violent extremism online. Where once we relied heavily on users to flag this content to us, today the majority of terrorist content we remove on Google products is first identified by our machines. We can then send this content to our language and subject matter experts, who swiftly and accurately review and remove content. We've also built systems that allow us to work in partnership with NGOs, other tech companies, and government Internet Referral Units, like Europol, to alert us to potentially problematic content."); *see also* Solon, *supra* note 31.

that industry partners and law enforcement have been notified.[144] The practice is reminiscent of how nation states often collaborate in publicly attributing cyberattacks to state actors.[145] One recent example is the large-scale takedown of accounts and pages associated with QAnon. YouTube made the move shortly after Facebook banned related users and content from its platform in October 2020.[146]

There also appears to be an open line of communication among platforms and government to share information, identify threats, synchronize policy responses, and coordinate with law enforcement.[147] Platforms at times explicitly state that government tips prompted their enforcement action. For instance, in September 2020, Facebook and Twitter said that they acted against a Russian-backed fake user network attempting to spread disinformation based

---

[144] *See, e.g.*, *August 2020 Coordinated Inauthentic Behavior Report*, *supra* note 92 ("In August, we removed three networks of accounts, Pages and Groups. Two of them—from Russia and the US—targeted people outside of their country, and another from Pakistan focused on both domestic audiences in Pakistan and also in India. We have shared information about our findings with law enforcement, policymakers and industry partners."); Devin Coldewey, *Facebook and Twitter Remove Hundreds of Accounts Linked to Iranian and Russian Political Meddling*, TECHCRUNCH (Aug. 21, 2018), https://perma.cc/EYV5-QKRD.

[145] *See, e.g.*, *The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China*, WHITE HOUSE BRIEFING ROOM (July 19, 2021), https://perma.cc/YQ3J-HDBU.

[146] *See An Update to How We Address Movements and Organizations Tied to Violence*, *supra* note 79; Nick Statt, *Facebook Completely Bans QAnon and Labels it a 'Militarized Social Movement'*, VERGE (Oct. 6, 2020), https://perma.cc/42W8-AWMB; The YouTube Team, *Managing Harmful Conspiracy Theories on YouTube*, YOUTUBE OFFICIAL BLOG (Oct. 15, 2020), https://perma.cc/58GN-KXEQ (notably, YouTube enforced against QAnon content prior to its October 2020 policy change banning conspiracy theories that could lead to physical harm). Twitter removed thousands of QAnon accounts as early as July 2020. *See* Bobby Allyn, *Twitter Removes Thousands of QAnon Accounts, Promises Sweeping Ban on the Conspiracy*, NPR (July 21, 2020), perma.cc/Y7UW-T9YQ.

[147] *See, e.g.*, *Atlantic Council Panel*, *supra* note 43 (remarks by Yoel Roth, Head of Site Integrity, Twitter) ("Several days before the [2018 U.S.] election a website went online that called itself IRA USA. . . . The website made a series of bold claims [concerning election interference] . . . . [W] e were able to respond to it rapidly, first by coordinating within industry to understand the extent of the activity we observed; second, by partnering with government to understand where is this activity coming from, who is behind it, what is the shape of the threat here. And then third, acting in a coordinated and decisive manner to address the activity across the board."); Huntley, *Protecting Users*, *supra* note 135 ("[Google's] TAG works closely with other technology companies—including platforms and specialized security firms—to share intelligence and best practices. We also share threat information with law enforcement. . . . Going forward, our goal is to give more updates on the attacks that TAG detects and stops. Our hope is that shining more light on these actors will be helpful to the security community, deter future attacks, and lead to better awareness and protections among high-risk targets.").

on an FBI tip. The operation was reportedly originally identified by U.S. intelligence agencies.[148] Twitter publicly thanked the FBI for providing intelligence about an Iran-based network that attempted to influence discourse about the 2020 U.S. presidential debates.[149] After the 2020 elections, platform executives said that "a number of our major takedowns were tipped by government partners."[150]

In other cases, platforms acted in proximity to similar government action, suggesting a possible connection between the actions. For example, Facebook and Twitter's mass deplatforming of accounts linked to the Russian IRA closely followed the designation and indictment of the group by the U.S. government. One month after the Treasury Department announced new IRA sanctions,[151] Facebook removed over one hundred IRA-associated accounts across its platforms.[152]

2. Long-Term Cooperative Institutions

In addition to ad hoc cooperation around specific incidents, platforms appear to be entrenching cooperation among themselves as well as with other stakeholders in certain critical policy areas by creating new institutions. Two key examples are the 2017 formation of the Global Internet Forum to Counter Terrorism (GIFCT) and platforms' periodic meetings with government agencies regarding election integrity in the framework of a designated working group.

The GIFCT is an initiative Facebook, Microsoft, Twitter, and YouTube spearheaded in response to pressure following major terrorist attacks that impacted platforms.[153] The live-streamed 2019 Christchurch terrorist attack

---

[148] Sheera Frenkel & Julian E. Barnes, *Russians Again Targeting Americans with Disinformation, Facebook and Twitter Say*, N.Y. TIMES (Sept. 1, 2020), https://perma.cc/ATY4-39FS.

[149] @TwitterSafety, TWITTER (Sept. 30, 2020, 5:26 PM), https://perma.cc/X9XH-VDJZ.

[150] *See* Stanford 2020 Election Panel, *supra* note 97, transcript at 17.

[151] *See Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the U.S. Political System*, U.S. DEP'T JUST. OFF. PUB. AFFS. (Feb. 16, 2018), https://perma.cc/Y8A8-5ZD2; *Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks*, U.S. DEP'T TREASURY (Mar. 15, 2018), https://perma.cc/GN39-DQDM.

[152] Josh Constine, *Facebook Reveals Russian Troll Content, Shuts Down 135 IRA Accounts*, TECHCRUNCH (Apr. 3, 2018), https://perma.cc/XG7T-URY2.

[153] *See Global Internet Forum to Counter Terrorism to Hold First Meeting in San Francisco,* FACEBOOK NEWSROOM (July 31, 2017), https://perma.cc/NT66-MSDZ; *see also* Evelyn Douek, *The Rise of Content Cartels,* KNIGHT FIRST AMENDMENT INSTITUTE, Feb. 2020, at 1, 8-10.

added impetus and urgency to this initiative.[154] Other tech companies have since joined the GIFCT. The GIFCT was established with significant international weigh-in from both government entities and NGOs.[155]

The GIFCT aims to foster and structure counterterrorism cooperation among industry players, civil society, academia, governments, as well as supra-national bodies such as the United Nations Counter-Terrorism Executive Directorate and the European Union.[156] The objective was "to engage in shared learning about terrorism," develop best practices for guidelines development and policy enforcement, and promote counter-speech in tandem with civil society on an international scale.[157] An important component of this initiative is the Industry Hash Database. Originally an EU Internet Forum tool, the database allows companies to create "digital fingerprints" for terrorist content and share it with other participating companies.[158]

In the areas of election integrity and influence operations, Facebook, Twitter, Google, and other platforms formed a working group with U.S. government agencies. The working group meets regularly.[159] Meetings took place as often as once a week in the period before the 2020 U.S. election.[160] Facebook's Head of Cybersecurity has said that the goal of these meetings "isn't necessarily to talk about specific instances, but to talk about the trends, the

---

[154] N.Z. Ministry Foreign Affs. & Trade, *The Call*, CHRISTCHURCH CALL: TO ELIMINATE TERRORIST AND VIOLENT EXTREMIST CONTENT ONLINE (May 15, 2019), https://perma.cc/S8HG-GDJ9.

[155] Twitter Public Policy, *Global Internet Forum to Counter Terrorism*, TWITTER BLOG (June 26, 2017), https://perma.cc/BM2S-UXMA ("The new forum builds on initiatives including the EU Internet Forum and the Shared Industry Hash Database; discussions with the UK government; and the conclusions of the recent G7 and European Council meetings.").

[156] *Id.*; *see also About*, GIFCT, https://perma.cc/FW4Y-XXCJ.

[157] Twitter Public Policy, *supra* note 155; *see also* Edgett Testimony, *supra* note 115, at 16-17 (noting, in the context of GIFCT, that Twitter has participated in more than 100 countering violent extremism training meetings and events around the world); Cruickshank, *supra* note 71, at 11 (highlighting Facebook's civil society outreach effort to counter violent extremism, including the "Peer to Peer" (P2P) Facebook Global Digital Challenge. P2P has launched more than five hundred counter-speech campaigns from students in sixty-eight countries).

[158] Google Public Policy, *Update on the Global Internet Forum to Counter Terrorism*, KEYWORD (Dec. 4, 2017), https://perma.cc/W7KR-AGTZ.

[159] *See* Facebook Newsroom (@fbnewsroom), *Sharing our joint industry statement on the latest meeting and collaboration between tech companies and USG agencies tasked with protecting the integrity of the election*, TWITTER (Sept. 16, 2020, 12:31 PM), https://perma.cc/JC5V-MARG; Twitter Public Policy (@Policy), TWITTER (Aug. 12, 2020, 12:38 PM), https://perma.cc/MF4M-ZVSV; *see also* Salvador Rodriguez, *The FBI Visits Facebook to Talk About 2020 Election Security, with Google, Microsoft and Twitter Joining*, CNBC (Sept. 4, 2019), https://perma.cc/GSJ2-M6E5.

[160] *See* Stanford 2020 Election Panel, *supra* note 97, transcript at 17.

challenges we're seeing in foreign interference, and to ask [whether] our industry [is] doing everything . . . to get ahead of this problem, and [whether] government [is] doing everything . . . and how we share information."[161] He expressed satisfaction with the work of the group and hope that it evolves from a voluntary forum into a more formal arrangement.[162] It is difficult, however, to evaluate the work of this group independently because we know very little about it beyond buzz-word laden one paragraph-long press releases and public commentary.[163]

B. Replicating Traditional Government Policy Approaches

The recent geopolitical and security turn of major platforms also manifests in the adoption of national security policy practices and tools that governments have employed for decades. Clearly, the policy options available to platforms are different than those available to states. Platforms can set standards and rules for their users, create and terminate business partnerships, and adjust technology. They can take various measures to control content on their platforms, including labeling, de-ranking, applying amplification restrictions, removing specific content, banning certain advertisements, or even deplatforming users and networks wholesale. But they lack government's coercive power, including the ability to use force.

Nevertheless, the menu of options available to the major technology platforms coupled with their role in modern society still gives them ample restrictive power and an ability to impose meaningful sanctions on individuals and groups. Platforms have wielded this power in part by transplanting frequently used government national security tools and methods into their own practice. The fact that many platform officials in trust and safety roles have previously held government national security posts has contributed to the importation of government practices and thinking into platform operations.[164]

---

[161] *See Atlantic Council Panel*, *supra* note 43 (remarks by Nathaniel Gleicher); *see also id.* (remarks by Yoel Roth, Head of Site Integrity, Twitter) ("[A]nd then finally . . . partnerships. A key part of how we prepare for elections around the world is not only working together as an industry but also ensuring collaboration with our stakeholders in governments, civil society and the research community. And we remain focused on that as a key part of how we respond to threats . . . going into the period immediately around the election.").

[162] *See* Stanford 2020 Election Panel, *supra* note 97, transcript at 17.

[163] *See* sources cited *supra* note 159.

[164] *See supra* Part II.B.

One area in which platforms have essentially replicated a well-established government policy approach to geopolitical and security threats is the designation and sanctioning of organizations and individuals, their associates and supporters.[165] This method mirrors a familiar U.S. government practice of designating individuals and groups for various sanctions to address national security threats.[166]

U.S. government designation mechanisms include dozens of sanctions programs. They target multiple states and transnational threats like malicious cyber activity, terrorism, and proliferation of weapons of mass destruction.[167] The United States also blacklists individuals for national security reasons via no-fly lists and other travel restrictions. Blacklists have even been compiled to identify targets for lethal counterterrorism strikes abroad.[168]

The designation process and its implications vary depending on the specific authority and context, but they all authorize government to single out individuals and groups for national security or geopolitical reasons, to impose sanctions based on that designation, and to pursue those *associated* with designated individuals and groups with additional sanctions. The same basic method drives platforms' enforcement policies against dangerous organizations and coordinated inauthentic behavior. Platforms curate lists of banned users and groups. In lieu of travel restrictions, asset freezes, and economic ostracization, this method translates in the world of platforms to content and access restrictions on users either due to their own conduct or because of their association with other users, groups, or networks. Platforms add their unique toolkit of sanctions to the economic or movement restrictions of government sanctions.

Both Facebook and Twitter's terms of service include a section on dangerous organizations and individuals that provides for designation and sanctioning of users. Facebook's community standards provide that "[i]n an

---

[165] *See* CHRIS MESEROLE & DANIEL BYMAN, RUSI & BROOKINGS, GLOBAL RESEARCH NETWORK ON TERRORISM AND TECHNOLOGY NO. 7: TERRORIST DEFINITIONS AND DESIGNATIONS LISTS: WHAT TECHNOLOGY COMPANIES NEED TO KNOW 2 (2019) ("Many technology companies refer to third-party terrorist definitions and designation lists when moderating potential terrorist accounts.").

[166] This is also a popular practice elsewhere in the world. *See*, *e.g.*, Elena Chachko, *Foreign Affairs in Court: Lessons from CJEU Targeted Sanctions Jurisprudence,* 43 YALE J. INT'L L. 1 (2019) (considering the use of foreign policy and national security designations in the European Union).

[167] *See infra* Part III.C. for more detailed discussion of U.S. sanctions authorities; *see also* Elena Chachko, *Administrative National Security*, 108 GEO. L.J. 1063, 1093-98 (2020).

[168] *See* Chachko, *supra* note 167, at 1093-98.

effort to prevent and disrupt real-world harm, we do not allow organizations or individuals that proclaim a violent mission or are engaged in violence to have a presence on Facebook."[169] This includes organizations or individuals involved in terrorist activity, organized hate, and organized violence. Facebook provides a non-exhaustive definition of organizations that fall under this rule.[170]

Facebook gradually expanded the enforcement of this policy from terrorist organizations that drew attention in earlier stages of Facebook's counterterrorism and counter violent extremism efforts—ISIS, al-Qaeda, and affiliates—to other terrorist groups, hate groups, and militarized organizations. It extended the policy to domestic groups like QAnon and participants of the January 6 insurrection.[171] Facebook's recently leaked Dangerous Individuals and Organizations list includes thousands of groups and individuals.[172]

Importantly, QAnon and other groups that Facebook and other platforms enforce against are not necessarily designated by the U.S. or other governments. The platform blacklisting enterprise involves a large degree of independent policy discretion. To mention another example, when Facebook deplatformed the Myanmar military over the February 2021 coup, it also banned linked commercial entities which it identified independently based on a UN report.[173]

Likewise, Twitter's rules and policies provide that "[t]here is no place on Twitter for violent organizations, including terrorist organizations, violent extremist groups, or individuals who affiliate with and promote their illicit

---

[169] *Dangerous Individuals and Organizations*, FACEBOOK TRANSPARENCY CTR., https://perma.cc/BA52-CMQ4.

[170] *Id.* Terrorist organizations and terrorists include any "non-state actor that: Engages in, advocates, or lends substantial support to purposive and planned acts of violence, [w]hich causes or attempts to cause death, injury or serious harm to civilians, or any other person not taking direct part in the hostilities in a situation of armed conflict, and/or significant damage to property linked to death, serious injury or serious harm to civilians [w]ith the intent to coerce, intimidate and/or influence a civilian population, government, or international organization [i]n order to achieve a political, religious, or ideological aim." The definition also extends to hate organizations, as well as the leaders and prominent members of such organizations.

[171] *See 2020 Dangerous Orgs Update*, *supra* note 76 ("When we started detecting hate organizations we focused on groups that posed the greatest threat of violence at that time, and we've now expanded to detect more groups tied to different hate-based and violent extremist ideologies and using different languages.").

[172] Sam Biddle, *Revealed: Facebook's Secret Blacklist of "Dangerous Individuals and Organizations"*, INTERCEPT (Oct. 12, 2021), https://perma.cc/CR4P-8MD4.

[173] Rafael Frankel, *An Update on the Situation in Myanmar*, FACEBOOK NEWSROOM (updated Apr. 14, 2021), https://perma.cc/U486-85SG.

activities."[174] The rules state that the platform's assessments in this context "are informed by national and international terrorism designations."[175] In addition to following government designations, Twitter has its own criteria.[176] The policy states that Twitter examines group activities both on and off the platform.[177] YouTube's community guidelines similarly ban content from violent or terrorist organizations. The platform's public rules on this issue, however, are more rudimentary and vague than those of Facebook and Twitter.[178]

Much like governments have done with their own designation mechanisms, platforms have extended the practice beyond just counterterrorism and preventing violent extremism.[179] The growing practice of identifying and taking down networks behind influence operations and other forms of inauthentic behavior is based on the very same logic.[180]

In sum, platforms replicate government sanctions lists and expand them. They add another layer to government economic or physical movement restrictions by imposing global restrictions on content and access to their products. As I show in previous work, government designation processes—often heavily based on classified material and loose criteria—have notorious due process deficits, and in the United States, they are exceedingly difficult to successfully challenge in court.[181] Although platforms must comply with

---

[174] *Violent Organizations Policy*, TWITTER HELP CTR. (Oct. 2020), https://perma.cc/QG7V-987G

[175] *Id.*

[176] *Id.* Twitter outlines three cumulative criteria: identification as an extremist group, engaging in violence or promoting violence as a means to further the group's cause, and targeting civilians.

[177] *Id*.

[178] *YouTube Policies: Violent Criminal Organizations*, YOUTUBE HELP, https://perma.cc/9RXV-UKLG. Google elaborates its policy on terrorist content in its transparency reports. The company states that "Content that violates our policies against violent extremism includes material produced by government-listed foreign terrorist organizations. We do not permit terrorist organizations to use YouTube for any purpose, including recruitment. YouTube also strictly prohibits content that promotes terrorism, such as content that glorifies terrorist acts or incites violence. . . . Content produced by violent extremist groups that are not government-listed foreign terrorist organizations is often covered by our policies against posting hateful or violent or graphic content." *Featured Policies*, GOOGLE TRANSPARENCY REP., https://perma.cc/L7KW-T6TM.

[179] *See* Chachko, *supra* note 167; Chachko, *supra* note 166.

[180] *See supra* Part II.B.

[181] *See* Chachko, *supra* note 167.

government-imposed sanctions against third parties,[182] they have gone beyond what is strictly required by law.[183] Platform amplification of government designations enhances the individual liberties harms folded into this government practice.[184]

C. The Function of Ambient Law

1. Constraining Legal Factors?

Where do the platform geopolitical and security policies and practices considered thus far meet U.S. domestic law?[185] Is there even any law to apply

---

[182] *See* discussion *infra* Part III.C.

[183] *See* Part III.C.2.

[184] On this point, see Robert Wright, *Why Is Facebook Abetting Trump's Reckless Foreign Policy?*, WIRED (May 7, 2019), https://perma.cc/GQ3J-B4Z6 ("So basically Trump can tell Facebook to de-platform any part of any foreign government—including, presumably, an entire foreign government—and [Facebook's head of Counterterrorism and Dangerous Organizations] Fishman, along with Facebook CEO Mark Zuckerberg, will reply with a crisp salute? Under Facebook's current policy, that would seem to be the case."); *see also* Part III.C.2.ii (addressing Facebook's blocking of the Iranian Revolutionary Guard Corps).

[185] There is no binding international law framework that applies directly to platform geopolitical and security practices. Generally, international law only applies to corporations after it is incorporated into the domestic law of the states in which they operate. *See, e.g.*, Jay Butler, *The Corporate Keepers of International Law*, 112 AM. J. INT'L L. 189, 199 (2020); José E. Alvarez, *Are Corporations "Subjects" of International Law?*, 9 SANTA CLARA J. INT'L L. 1 (2011); John H. Knox, *Horizontal Human Rights Law*, 102 AM. J. INT'L L. 1 (2008). The international law of state responsibility allows attribution of corporate action to a state under certain conditions, but even then, the state remains the bearer of the international obligation and the party responsible for its violation under international law. *See Draft Articles on Responsibility of States for Internationally Wrongful Acts*, 2 Y.B. Int'l L. Comm'n 26, U.N. Doc. A/56/10/2001 (2001). On attribution in cyberspace under international law, see also Eichensehr, *supra* note 22.

Nevertheless, corporations often voluntarily undertake to comply with international law obligations, even when their own states are not bound by those obligations or explicitly reject them. *See* Butler, *supra*, at 203-14. Platforms have recently invoked international human rights law language as well. *See* Richard Allan, *Hard Questions: Where Do We Draw the Line on Free Expression?*, FACEBOOK NEWSROOM (Aug. 9, 2018), https://perma.cc/8NK2-FFHF; Monika Bickert, *Updating the Values That Inform Our Community Standards*, FACEBOOK NEWSROOM (Sept. 12, 2019), https://perma.cc/Y8UP-ZFJW; *Q & A with Facebook on Myanmar*, OPINIO JURIS (Sept. 20, 2020), https://perma.cc/MP3H-YBAL; @Jack, TWITTER (Aug. 10, 2018, 12:58 PM), https://perma.cc/8Y8D-BMEY. Importantly, Facebook's Oversight Board has drawn extensively on international human rights law in the cases it decided to date. *See An Empirical Look at the Facebook Oversight Board*, LAWFARE, https://perma.cc/PXQ5-N3GH. Platform recourse to international law is a relatively recent development, and one that has

to these practices? After all, we are largely concerned here with how private actors self-regulate to conduct their security and geopolitical affairs: how they organize their security and policy bureaucracies, how they develop their policies, how they enforce them against users, and how they collaborate with other stakeholders—domestic and international, governmental and non-governmental.

To be sure, there is plenty of restrictive federal and state law that governs various aspects of platform operations, either directly or indirectly. Trademark and copyright law,[186] various privacy requirements,[187] law pertaining to data handling,[188] general corporate, antitrust, and criminal law, and other bodies of domestic law all apply to platforms, and platforms must comply or face sanctions.

Nevertheless, existing statutory and administrative frameworks generally do not regulate the core platform geopolitical and security practices analyzed in the previous sections. Even certain statutes that regulate private actors specifically to protect security and geopolitical interests, like the Foreign Corrupt Practices Act of 1977 (FCPA) [189] and the Committee on Foreign

---

attracted much commentary. *See* David Kaye (Special Rapporteur for Freedom of Opinion and Expression), *Promotion and Protection of the Right to Freedom of Opinion and Expression on His Mission to Liberia*, U.N. Doc. A/HRC/38/35 (June 18, 2018); Barrie Sander, *Freedom of Expression in the Age of Online Platforms: The Promise and Pitfalls of a Human Rights-Based Approach to Content Moderation*, 55 FORDHAM INT. L.J. 939 (2020); Evelyn Aswad, *The Future of Freedom of Expression Online,* 17 DUKE L. & TECH. REV. 26 (2018); ELIŠKA PÍRKOVÁ & JAVIER PALLERO, ACCESS NOW, 26 RECOMMENDATIONS ON CONTENT GOVERNANCE: A GUIDE FOR LAWMAKERS, REGULATORS, AND COMPANY POLICY MAKERS (2020); evelyn douek, *The Limits of International Law in Content Moderation*, 6 U.C. IRVINE J. INT'L TRANSNAT'L & COMP. L. 37 (2021); Susan Benesch, *But Facebook's Not a Country: How to Interpret Human Rights Law for Social Media Companies*, YALE J. ON REG. BULLETIN (Sept. 14, 2020); Michael Lwin, *Applying International Human Rights Law for Use by Facebook,* YALE J. ON REG. BULLETIN (Sept. 14, 2020). For the moment, however, platforms' adherence to international obligations is impressionistic and aspirational—not legalistic. They have invoked the language of international human rights law when discussing the "values" that inform their content moderation rules—not as binding law in any formal sense.

[186] *See, e.g.*, The Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (1998); s*ee also, e.g.*, Katharine Trendacosta, *Reevaluating the DMCA 22 Years Later: Let's Think of the Users*, ELEC. FRONTIER FOUND. (Feb. 12, 2020).

[187] *See, e.g.*, In re Google Inc., 806 F.3d 125 (3d Cir. 2015); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COLUM. L. REV. 583 (2014).

[188] *See, e.g.*, The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712.

[189] 15 U.S.C. §§ 78dd-1-78dd-3. The FCPA, as amended, makes it unlawful for private actors to make payments to foreign government officials to secure improper business advantages. It is the main U.S. international business anti-corruption norm. The FCPA prohibits bribes to

Investment in the United States (CFIUS) mechanism,[190] are only peripherally relevant to these practices.[191]

---

secure any improper business advantage, not just monetary benefits. It provides for various sanctions. For an overview of the FCPA, see NICOLE VANATKO, CONG. RSCH. SERV., IF11588, THE FOREIGN CORRUPT PRACTICES ACT: AN OVERVIEW (2020); *see also* Amy Deen Westbrook, *Enthusiastic Enforcement, Informal Legislation: The Unruly Expansion of the Foreign Corrupt Practices Act*, 45 GA. L. REV. 489 (2011); *SEC Enforcement Actions: FCPA Cases*, U.S. Sec. & Exch. Comm'n, https://perma.cc/4WRH-RZZ3 (last updated Sept. 29, 2021) (detailing the SEC's FCPA Enforcement Actions). Despite criticism that the FCPA places U.S. companies at a disadvantage compared to foreign companies not subject to its provisions and ignores the prevalence of corruption in many parts of the world, FCPA enforcement has only increased over the years. *See* Rebecca L. Perlman & Alan O. Sykes, *The Political Economy of the Foreign Corrupt Practices Act: An Exploratory Analysis,* 9 J. LEGAL ANALYSIS 153 (2017).

[190] *See generally* JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (CFIUS) (2020). CFIUS is an interagency review of certain "mergers, acquisitions, or takeovers" that involve foreign investment in the United States. It operates pursuant to Section 721 of the Defense Production Act of 1950, as amended. 50 U.S.C. § 4565; *see also* 31 C.F.R. §§ 800-801 (2020). Section 721 grants the president the authority to prohibit such transactions or impose certain conditions if he finds that they jeopardize national security. The president has delegated that power to CFIUS through Executive Order 11,858. Foreign investment in the United States, Exec. Order. No. 11,858, 40 Fed. Reg. 20263 (May 7, 1975), *amended by* Exec. Order. No. 13,456, 73 Fed. Reg. 4677 (Jan. 25, 2008). With support from the Trump administration, in 2018, Congress passed comprehensive legislation to "modernize" the CFIUS process. The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) bolstered the CFIUS mechanism and strengthened its powers to address national security threats. *See* Stephanie Zable, *The Foreign Investment Risk Review Modernization Act of 2018*, LAWFARE (Aug. 2, 2018), https://perma.cc/637U-DLZW. A major driving force behind this legislation was concern that Chinese and other foreign actors would invest in U.S. companies that deal in advanced technologies or control critical technological infrastructure. This would allow foreign state competitors to gain access to such technologies, create risks to U.S. national security, and further challenge U.S. technological leadership. *See* JACKSON, *supra,* at 1-2; *see also* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 31 C.F.R. § 800 (2020) (modifying the mandatory declaration provision for certain foreign investment transactions involving a U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies.).

[191] One could imagine various potential scenarios in which the FCPA could intersect with platforms' geopolitical policymaking and execution. The FCPA applies not just to bribes in the form of payment, but also to anything deemed to be "of value." 15 U.S.C. §§ 78dd-1-78dd-3. However, the FCPA applies to a very specific potential form of platform behavior—bribing foreign officials to get something in return. The bulk of the practices described in the previous sections do not inherently involve such conduct.

The CFIUS mechanism affects the geopolitical and security calculations of foreign-controlled platforms. *See* 31 C.F.R § 800.252(a) (2020) ("The term U.S. business means any entity, irrespective of the nationality of the persons that control it, engaged in interstate commerce in the United States."). It also affects U.S. platforms considering foreign investment. Still, CFIUS has little direct bearing on the kinds of security and geopolitical

Similarly, constitutional obligations that could constrain platforms acting in the security and geopolitical space are at present inapplicable to the relationship between platforms and their users as a matter of law. Despite significant scholarly debate about requiring platforms to adhere to constitutional obligations such as the First Amendment and procedural due process, extant law continues to preclude such application.[192] Courts have generally declined to utilize the state action doctrine—which imposes certain public law obligations on private actors when they perform state-like functions—to subject platforms to constitutional duties.[193]

Consequently, these various legal frameworks do not regulate in any detail the subset of platform activities, still peripheral in the general scheme of their operations, that relate to monitoring and addressing geopolitical matters and security threats such as terrorism and violent extremism, influence operations, election integrity, and a global pandemic. They do not meaningfully constrain practices like intelligence synthesis, threat analysis, related information

---

practices described in the previous sections. Platform practices such as intelligence gathering, information sharing and other forms of international cooperation, both bilateral and multilateral, and enforcement against users who violate platform policies do not involve the kinds of commercial transactions that would trigger CFIUS review. They do not constitute a "merger, acquisition, or takeover . . . by or with any foreign person that could result in foreign control of any United States business." 50 U.S.C. § 4565(a)(4).

[192] *See* Manhattan Cmty. Access Corp. v. Halleck, 139 S. Ct. 1921 (2019); Prager Univ. v. Google LLC, 951 F.3d 991 (9th Cir. 2020); Doe v. Google LLC, No. 20-CV-07502-BLF, 2021 U.S. Dist. LEXIS 201377 (N.D. Cal. Oct. 19, 2021) (dismissing First Amendment claims against Google and declining to find state action); Tulsi Now, Inc. v. Google LLC, 2020 WL 4353686, at *2 (C.D. Cal. Mar. 3, 2020) ("What Plaintiff fails to establish is how Google's regulation of its own platform is in any way equivalent to a governmental regulation of an election. Google does not hold primaries, it does not select candidates, and it does not prevent anyone from running for office or voting in elections. To the extent Google 'regulates' anything, it regulates its own private speech and platform. Plaintiff's 'national security' argument similarly fails. Google protects *itself* from foreign interference; it does not act as an agent of the United States. . . . Google's self-regulation, even of topics that may be of public concern, does not implicate the First Amendment.").

[193] *See also, e.g.*, Klonick, *supra* note 18, at 1610 ("For a long time, the claim that online intermediaries are state actors or perform a public function and, thus, are subject to providing free speech guarantees, was a losing one."); Jonathan Peters, *The "Sovereigns of Cyberspace" and State Action: The First Amendment's Application—or Lack Thereof—to Third Party Platforms*, 32 BERKELEY TECH. L.J. 989 (2017) (reviewing related literature); Martha Minow, *Alternatives to the State Action Doctrine in the Era of Privatization, Mandatory Arbitration, and the Internet*, 52 HARV. C.R.-C.L. L. REV. 145 (2017); Daphne Keller, *Aegis Series No. 1902*, *Who Do You Sue? State and Platform Hybrid Power Over Online Speech*, HOOVER INST. (2019).

sharing, policy development, or platforms' enforcement methods against security threats.

At the same time, several domestic law elements boost and facilitate platforms' geopolitical and security practices. The combination of the absence of direct legal constraint and the existence of facilitating legal mechanisms creates a legal environment that allows platform-government cooperation around geopolitics and security to flourish. The next section explores enabling legal factors.

2. Enabling Legal Factors

i. Section 230 of the CDA

The cornerstone of the existing legal framework that allows platforms a wide margin of discretion in moderating user-generated content and developing related policies is the widely discussed and frequently criticized Section 230 of the Communications Decency Act.[194] Section 230 precludes platform liability for most user-generated content. This protection allows platforms to self-regulate and moderate content by enforcing against users who violate their rules or abstaining from enforcement without fear of endless litigation.[195]

Section 230 has been the subject of intense criticism of late, including both political attacks demanding that it be revoked and expert calls for reform.[196]

---

[194] 47 U.S.C. § 230.

[195] *See* Reno v. ACLU, 521 U.S. 844 (1997) (striking down Section 230's anti-indecency provisions but preserving its immunity provisions); Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997) (interpreting Section 230 as granting broad immunity to online content intermediaries to encourage self-regulation); *see also* Klonick, *supra* note 18, at 1606-09. For in-depth analysis of Section 230, see, for example, JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019); Mary Graw Leary, *The Indecency and Injustice of Section 230 of the Communications Decency Act*, 41 HARV. J.L. & PUB. POL'Y 553 (2018); VALERIE C. BRANNON ET AL., CONG. RSCH. SERV., LSB10484, SECTION 230 AND THE EXECUTIVE ORDER ON PREVENTING ONLINE CENSORSHIP (2020) [hereinafter SECTION 230 CRS REPORT]; Kate Klonick, *Everything You Need to Know About Section 230*, LAWFARE (July 17, 2020); https://perma.cc/RWF2-Y5CN; Matt Reynolds, *The Strange Story of Section 230, the Obscure Law that Created Our Flawed, Broken Internet*, WIRED (Mar. 24, 2019), https://perma.cc/9F3S-HAYX; Daphne Keller, *Toward a Clearer Conversation About Platform Liability*, KNIGHT FIRST AMEND. INST. (Apr. 6, 2018), https://perma.cc/TL7X-LG7X.

[196] *See* Danielle Keats Citron & Benjamin Wittes, *The Problem Isn't Just Backpage: Revising Section 230 Immunity*, 2 GEO. L. TECH. REV. 453 (2018); Jeff Kosseff, *Defending Section 230: The*

Some judges have also called for a reevaluation of the scope of Section 230 immunity to compel platforms to address harmful uses of their technology, particularly those that facilitate terrorism and other national security threats.[197] The main point for our purposes is that Section 230 has created a legal space in which platforms are currently allowed to address violative and dangerous content or conduct within their purview largely as they see fit. Section 230 shields these practices by protecting platforms from legal liability. If future congressional Section 230 reform follows recent judicial recommendations, it would lead to more—not less—platform enforcement in the geopolitical and security space.

ii. Sanctions and Other National Security Trade Restrictions

Economic sanctions and other trade restrictions that the U.S. government imposes on foreign relations and national security grounds constrain platforms the same way they constrain any other private actor. But in an environment in which platforms increasingly feel compelled to proactively contain negative

---

Value of Intermediary Immunity, 15 J. TECH. L. & POL'Y 123, 124 (2010); SECTION 230 CRS REPORT, *supra* note 195; Gilad Edelman, *Finally, an Interesting Proposal for Section 230 Reform*, WIRED (Feb. 5, 2021), https://perma.cc/GAF7-8428; Christiano Lima, *How a Widening Political Rift Over Online Liability Is Splitting Washington*, POLITICO (July 9, 2019), https://perma.cc/44SW-367C.

[197] *See* Force v. Facebook, Inc., 934 F.3d 53, 77 (2d Cir. 2019), (Katzman, C.J., concurring in part and dissenting in part) ("Instead, we today extend a provision that was designed to encourage computer service providers to shield minors from obscene material so that it now immunizes those same providers for allegedly connecting terrorists to one another. Neither the impetus for nor the text of [Section 230] requires such a result. . . . In light of today's decision and other judicial interpretations of the statute that have generally immunized social media companies—and especially in light of the new reality that has evolved since the CDA's passage—Congress may wish to revisit the CDA to better calibrate the circumstances where such immunization is appropriate . . . in light of congressional purposes."), *cert. denied*, 140 S. Ct. 2761 (2020). Chief Judge Katzman would distinguish platforms' role as hosts of third-party content, for which they are immune under Section 230, from other functions such as recommendation algorithms, for which they should not be.

In *Gonzalez v. Google LLC*, 2 F.4th 871, 939-40 (9th Cir. 2021), Judge Gould, dissenting in part, declined to find that Section 230 precluded certain claims based on Google, Twitter and Facebook's role in facilitating terrorist attacks. He maintained that "regulation of social media companies would best be handled by [Congress and the Executive], but that in the case of sustained inaction by them, the federal courts are able to provide a forum responding to injustices . . . . Here, that means . . . that the courts should be able to assess whether certain procedures and methods of the social media companies have created an unreasonably dangerous social media product." 2 F.4th at 919. Judge Berzon's concurrence endorsed Chief Judge Katzman's *Force v. Facebook* dissent and called on Congress to act. *Id.* at 913.

security and geopolitical implications of user activity,[198] sanctions also have an important enabling function. Government sanctions lists are a resource that platforms can replicate and expand upon in their own enforcement activity. They help compensate for platform expertise and capacity gaps in identifying bad actors. They provide political cover because platforms can justify their own enforcement action by arguing that they relied on authoritative government determinations that certain groups and individuals engage in unlawful activity or pose a national security risk.

U.S. trade law is rife with authority to impose national security trade restrictions and barriers.[199] One form of national security trade restriction germane to the operations of technology companies is the Commerce Department's Entity List, which subjects persons and entities to special export licensing requirements for national security reasons.[200] Another widely deployed method is the growing use of individual economic sanctions.[201] Several statutes authorize such sanctions, including the 1977 International Emergency Economic Powers Act (IEEPA),[202] the Antiterrorism and Effective

---

[198] *See supra* Part II.A.

[199] *See* Kathleen Claussen, *Trade's Security Exceptionalism,* 72 STAN. L. REV. 1097 (2020); *see also* Heath, *supra* note 17 (providing an international perspective on security exceptions and trade architecture).

[200] The Department's Bureau of Industry and Security (BIS) has published the Entity List since 1997. The grounds for inclusion in the Entity List are activities designated by the State Department and ones that are contrary to U.S. national security and foreign policy interests. *Entity List*, BUREAU INDUS. & SEC., U.S. DEP'T COM., https://perma.cc/56Y6-74MS. The Export Administration Regulations (EAR) govern the Entity List. *See* 15 C.F.R. § 744 (2020).

The Entity List has recently been used to restrict exports to Chinese technology companies. For instance, in 2019, BIS added Huawei Technologies and 114 of its affiliates to the List. In May 2020, the agency took additional action against the company over its alleged effort to circumvent restrictions imposed after its inclusion in the List. Press Release, U.S. Dep't Com., Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies (May 15, 2020), https://perma.cc/5F5U-JYSA. BIS also listed entities affiliated with Chinese telecom company ZTE. 15 C.F.R. § 744 (2016).

[201] *See* Chachko, *supra* note 167, at 1093-99.

[202] International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1707; National Emergencies Act, 50 U.S.C. §§ 1601–1651. IEEPA is the most frequently used authority for imposing economic sanctions. The statute empowers the president to take extensive economic measures in response to an "unusual and extraordinary" threat to the national security, foreign policy, or economy of the United States if the president declares a national emergency. 50 U.S.C. §1701(a). That authority extends not just to foreigners but also to U.S. persons. Beginning in the early 1990s, presidents invoked IEEPA not only against states but also to address transnational threats such as the proliferation of weapons of mass

Death Penalty Act of 1996 (AEDPA),[203] which governs Foreign Terrorist Organization (FTO) designations,[204] and other specific statutes.[205]

IEEPA and other economic sanctions, FTO designations under AEDPA, and Entity List restrictions reach many aspects of platform operations. They prohibit platforms from doing business with designated actors and determine what procedure they need to follow if they choose to export technology to Entity List designees.[206] However, it is not entirely clear what these designations and restrictions mean for what happens *on* the platforms. Must a platform remove all content posted by a person or entity subject to economic sanctions under IEEPA or AEDPA? Must it block their accounts? Would sharing ad revenue with terrorist content creators constitute material support for terrorism, which could violate a criminal prohibition[207] and expose platforms to civil liability?[208]

---

destruction, terrorism, and narcotics trafficking. After 9/11, the United States expanded the practice in those areas and beyond. Individual economic sanctions have played a significant role in U.S. policy on Russia, election meddling, and cybersecurity. The United States has also imposed sanctions related to threats from Iran, North Korea, Syria, Belarus, Burundi, Central African Republic, Congo, Iraq, Lebanon, Libya, Somalia, Sudan, Yemen, Venezuela, and Zimbabwe. Thousands of individuals and entities have been designated under these policies. *See* Chachko, *supra* note 167, at 1093-99.

[203] Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (1996).

[204] 8 U.S.C. § 1189(a)(1) (stating that a group may be designated an FTO if it is foreign and engages in terrorist activity that threatens the United States or its nationals). 8 U.S.C. § 1189(a)(2)(C) (stating that the Treasury may freeze an FTO's assets, those providing it material support may face criminal sanctions, and its alien members may be denied U.S. admission).

[205] *See, e.g.*, Countering America's Adversaries Through Sanctions Act, Pub. L. No. 115-44, 131 Stat. 886 (2017); Exec. Order No. 13,849, 83 Fed. Reg. 48, 195 (2018) (concerning Russia, Iran, and North Korea). The implications of sanctions vary according to the designation authority. Generally, IEEPA designations involve the freezing of the assets of the designated person within U.S. jurisdiction and restrictions on doing business with them. Those who deal with designated persons, including U.S. persons who do so, risk being designated themselves. Moreover, executive orders pursuant to IEEPA provide civil and criminal penalties for those who violate or conspire to violate sanctions. Similarly, after the State Department designates an FTO under AEDPA, the Treasury Department may—but is not required to—block its assets, those providing it material support may face criminal sanctions under the material support statute (*see* 18 U.S.C. § 2339B), and financial institutions must report FTO assets. On the implications of designations under each authority, see Elena Chachko, *The U.S. Names the Iranian Revolutionary Guard a Terrorist Organization and Sanctions the International Criminal Court,* LAWFARE (Apr. 10, 2019), https://perma.cc/4XU8-B2X6.

[206] *See* sources cited *supra* notes 202-203.

[207] 18 U.S.C. § 2339A.

[208] 18 U.S.C. § 2333.

What about allowing ISIS to reach supporters by recommending ISIS accounts to users?[209]

Several courts have recently addressed these questions in cases brought under the Anti-Terrorism Act (ATA), which imposes civil liability for material support for acts of international terrorism.[210] Appellate courts have reaffirmed that Section 230 of the CDA grants platforms extensive immunity from liability not only for content but also for the output of their recommendation and ad algorithms.

In *Force v. Facebook*, the Second Circuit Court of Appeals affirmed the dismissal of a lawsuit by terrorism victims alleging that Facebook provided material support to Hamas, a designated FTO, by hosting Hamas content and facilitating Hamas recruiting by recommending Hamas accounts. The Second Circuit held that Section 230 barred the plaintiffs' claims, and the Supreme Court denied certiorari.[211] Chief Judge Katzman, dissenting in part, would deny Section 230 immunity for claims concerning Facebook's recommendation algorithms. He called on Congress to limit Section 230 immunity for functions that facilitate terrorism and other harms.[212]

A similar 9th Circuit case, *Gonzalez v. Google*,[213] grew out of ISIS-linked attacks in Paris, Istanbul, and San Bernardino. Victims sued Google, Facebook, and Twitter pursuant to the ATA for hosting and recommending ISIS content to users, funneling a percentage of advertisement revenue to creators of ISIS videos, and allowing ISIS affiliates to connect and organize on their platforms. The majority again found that Section 230 of the CDA barred most of the plaintiffs' claims. Nevertheless, the Court held that Section 230 does not categorically bar Google's liability for sharing advertisement revenue with ISIS affiliates.[214] The concurrences again called for Section 230 reform along the lines of the *Force v. Facebook* dissent.[215]

---

[209] On the applicability of material support statutes to online freedom of speech issues, see Rachel E. VanLandingham, *Jailing the Twitter Bird: Social Media, Material Support to Terrorism and Muzzling the Modern Press*, 39 CARDOZO L. REV. 1 (2017); KATHLEEN ANN RUANE, CONG. RSCH. SERV., R44626, THE ADVOCACY OF TERRORISM ON THE INTERNET: FREEDOM OF SPEECH ISSUES AND MATERIAL SUPPORT STATUTES (2016).

[210] 18 U.S.C. § 2333.

[211] Force v. Facebook, Inc., 934 F.3d 53 (2d Cir. 2019), *cert. denied*, 140 S. Ct. 2761 (2020).

[212] *See* sources cited *supra* note 197.

[213] Gonzalez v. Google LLC, 2 F.4th 871, 890 (9th Cir. 2021).

[214] 18 U.S.C. § 2333(a), (d).

[215] *See Gonzales*, 2 F.4th at 913; *id.* at 918 (Gould, J., concurring in part and dissenting in part).

Despite platforms' broad immunity from material support claims based on content and recommendations, it appears that platforms remove content under their own dangerous organizations and other relevant policies out of an abundance of caution.[216] For instance, when the U.S. government designated the Iranian Revolutionary Guard Corps (IRGC) as an FTO under AEDPA, Facebook removed content posted by IRGC affiliates from Instagram even though it remains an open question whether merely hosting FTO content constitutes material support for terrorism.[217] As we saw, courts have precluded civil liability, and the question of whether platform-hosted content constitutes material support for purposes of the criminal material support statute has yet to be tested in court.[218] This example illustrates that government sanctions lead platforms to enforce against users beyond what the law strictly requires.

As Part III.B shows, platforms have replicated the method of designating individuals and groups for sanctions on security and geopolitical grounds. Like government, they now curate lists of banned users and subjects of increased monitoring. They rely on U.S. and other government sanctions in identifying groups and individuals for enforcement action.[219] They expand government lists by applying their own designation criteria and exercise independent judgement as to which users to enforce their policies against. In other words, sanctions laws facilitate and enhance platforms' own blacklisting practices.

iii. Formal and Informal Law Enforcement and National Security Data Sharing

A variety of laws allow government agencies to obtain user data from technology companies. Like any other entity, platforms must comply with lawful subpoenas, warrants, and court orders that require such disclosure,[220]

---

[216] Wright, *supra* note 184 ("When I asked Fishman [Facebook's head of Counterterrorism and Dangerous Organizations] to justify this policy, he said it's designed to keep Facebook on the right side of the law, which prohibits Americans from providing 'material support' to any group deemed a 'Foreign Terrorist Organization.'").

[217] *See* Golnaz Esfandiari, *Instant Ban for Iran's IRGC On Instagram: Social-Media Giant Blocks Commanders' Sites*, RADIO FREE EUR. (Apr. 17, 2019), https://perma.cc/RC7H-ECGS.

[218] *See also Gonzalez*, 2 F.4th at 890; Force v. Facebook, Inc., 934 F.3d 53, 71-72 (2d Cir. 2019) (clarifying that the holding that there is no civil liability for content or recommendation algorithms under the ATA does not bar criminal prosecution under 18 U.S.C. § 2339B), *cert. denied*, 140 S. Ct. 2761 (2020).

[219] *See supra* Parts III.A.2, III.B.

[220] *See* Rozenshtein, *supra* note 18, at 122-34.

including requests under the Foreign Intelligence Surveillance Act (FISA).[221] Scholars have identified ways in which platforms push back against government secrecy requirements and law enforcement assistance requests.[222] Platforms can and have challenged action they viewed as government overreach using various techniques.[223] As Alan Rozenshtein observes, these methods of resistance belie "the common assumption that the government always gets its way" and that technology companies that contribute to government surveillance "operate under a 'regime of automatic compliance.'" [224] Nevertheless, platforms comply with the majority of government requests.[225]

In addition, several authorities outline either non-judicial or voluntary disclosure procedures specifically in the area of national security. One example is National Security Letters (NSLs). NSLs are generally issued by the FBI to obtain information from companies to advance national security investigations. Recipients of such requests are subject to a secrecy requirement and are not allowed to disclose them to the public.[226] Platforms and rights advocates have attempted to push back against the secrecy requirement but have largely been

---

[221] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 50 U.S.C.).

[222] *See* Deeks, *supra* note 18; Rozenshtein, *supra* note 18.

[223] Rozenshtein, *supra* note 18. Rozenshtein identifies several techniques that technology companies have employed to push back against government requirements: proceduralism and litigiousness, technological unilateralism, and policy mobilization. *Id.* at 122-44. *Cf.* Michaels, *All the President's Spies*, *supra* note 22, at 923 ("A legalistic, transactional relationship with a corporation, in which the firm cooperates only to the extent a court order or subpoena specifies, is likely to inhibit the type of open-ended, fast-moving collaboration that the intelligence agencies prefer.").

[224] Rozenshtein, *supra* note 18, at 125.

[225] *See Requests for User Information FAQs*, GOOGLE TRANSPARENCY REP. HELP CTR., https://perma.cc/8JB5-ELLP; *Government Requests to Remove Content: Government Removal Requests by the Numbers: United States*, GOOGLE TRANSPARENCY REP., https://perma.cc/3BES-N45L; *Government Requests for User Data: United States*, FACEBOOK TRANSPARENCY CTR., https://perma.cc/FV4K-YGUQ; *Information Requests*, TWITTER TRANSPARENCY, https://perma.cc/39U9-82GT.

[226] 18 U.S.C. § 2709(a), (c). *See* Hannah Bloch-Wehba, *Process Without Procedure: National Security Letters and First Amendment Rights*, 49 SUFFOLK U. L. REV. 367, 367 (2016) ("Each year, the FBI uses tens of thousands of NSLs to obtain customer . . . transactional records—such as records related to telephone calls, emails, text messages, online forums, tweets, or Facebook messages—from service providers."); Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2332 (2014).

denied by courts.[227] Another example is voluntary disclosure under the Stored Communications Act (SCA). Among other provisions related to government information requests, [228] the SCA permits the voluntary disclosure of communications content "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." [229] Google, Facebook and Twitter publish transparency reports detailing government requests they receive, with separate reporting on requests made under national security laws.[230]

Other statutory provisions address informal cybersecurity information sharing. The Cybersecurity Information Sharing Act of 2015 encourages—but does not compel—private companies to share information about cyber threat indicators and related defensive measures by granting them certain protections for such disclosure.[231] The Cybersecurity and Infrastructure Security Agency Act of 2018 (CISAA 2018), [232] which reorganized the Department of Homeland Security by creating the Cybersecurity and Infrastructure Agency, also calls for public-private information sharing. For example, Section 2202 of CISAA 2018 authorizes the Secretary for Homeland Security to coordinate various aspects of cyber policy with the private sector and to synthesize information originating in the private sector.[233] Section 2202 highlights counterterrorism information sharing, but, as we have seen, the Department of Homeland Security has been

---

[227] *See, e.g.*, Twitter, Inc. v. Barr, 445 F. Supp. 3d 295 (N.D. Cal. 2020), *appeal filed*, No. 20-16174 (9th Cir. June 16, 2020); Twitter, Inc. v. Holder, 183 F. Supp. 3d 1007, 1009, 1014 (N.D. Cal. 2016). *But see* Microsoft Corp. v. U.S. Dep't of Just., 233 F. Supp. 3d 887 (W.D. Wash. 2017); Brad Smith, *DOJ Acts to Curb the Overuse of Secrecy Orders. Now It's Congress' Turn,* MICROSOFT: MICROSOFT ON THE ISSUES (Oct. 23, 2017), https://perma.cc/A6NL-3V2L (describing a Microsoft challenge to government gag orders for data requests under the Stored Communications Act).

[228] *See, e.g.*, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (finding that Microsoft's challenge to a government warrant under the Stored Communications Act (18 U.S.C. § 2703) to produce data stored in Ireland moot after Congress passed the CLOUD Act); *see also* Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

[229] 18 U.S.C. § 2702(b)(8).

[230] *Supra* note 225.

[231] 6 U.S.C. §§ 1501–1510.

[232] 6 U.S.C. §§ 651–674.

[233] *Id.*

engaged in continuous cooperation and information sharing with platforms on matters of election security as well.[234]

Voluntary information sharing provisions such as the ones discussed here lubricate platform efforts to cooperate with government to identify and combat threats to their products in contexts such as influence operations and counterterrorism. Although platforms have made efforts in recent years to draw attention to their resistance to certain government data and content requests, [235] the previous sections show that they have cooperated with government on these matters extensively. Statutory provisions that encourage informal private-public information sharing on security and geopolitical issues facilitate, rather than constrain, such practices.

Existing law allows platforms to engage in geopolitical and security practices and self-regulate in this context without meaningful legal constraint. At the same time, several legal factors bolster these platform practices and create avenues for informal cooperation with government around them.

IV. NATIONAL SECURITY BY PLATFORM AS PRIVATIZATION

Thus far, we explored the rise of the geopolitics and security bureaucracies of major platforms, their methods and practices, and their relationship with government. That relationship involves threat analysis and policy development cooperation, information sharing, and platforms replicating government practices and methods. A mutually beneficial, at times even symbiotic, relationship has emerged between platforms and government agencies in addressing certain important national security and geopolitical challenges. On other fronts, however, platforms and government have clashed. Ambient law does little to constrain these practices and interactions. In fact, it often facilitates and enables them.

---

[234] *See Atlantic Council Panel*, *supra* note 43; Brookings Panel, *supra* note 68.

[235] *See* Rozenshtein, *supra* note 18; Deeks, *supra* note 18. To take an example from a different jurisdiction, during the spring 2021 clash between Israel and Gaza and sectarian violence within Israel, the Israeli government disclosed data about its national security content takedown requests to platforms and their acceptance rates. Facebook accepted only 46% of the requests, while Instagram accepted only 41%. Other platforms were far more cooperative. Twitter accepted 82% of the requests, and TikTok accepted 89%. There was no data on YouTube's disposition of removal requests. Israel Office of the State Attorney, FACEBOOK (May 19, 2021, 7:42 PM), https://perma.cc/MF3Q-4NWZ. The Israeli Supreme Court recently sanctioned the practice of informal takedown requests by the State Attorney's office to platforms. *See* HCJ 7846/19 Adalah v. Israel Office of the State Attorney __ PD __ (Apr. 12, 2021) (Isr.), https://perma.cc/2MUN-P5YZ.

This Part proposes to understand and think about these trends as instances of indirect, informal national security privatization. Subpart B examines national security by platform through the lens of privatization theory. Before turning to the theoretical discussion, Subpart A offers a descriptive typology of the emerging platform-government national security and geopolitical nexus. The typology breaks down national security by platform into three analytically distinct privatization modes. Each mode deviates from the privatization paradigm along similar lines, but also has unique drivers, features and implications for the government-platform national security and geopolitical relationship.

A. Mapping Privatization Categories

Situations in which informal privatization of national security powers to platforms has occurred to date can be analyzed under three main categories: (1) *hard structural constraints*; (2) *bureaucratic workarounds*; (3) *platforms as substitutes.* More than one category may apply to a single area of platform-government security or geopolitical interactions. In some interactions the interests of platforms and government align. In others they may conflict. In yet others, platforms have built coalitions with certain players within government even as other key government actors' preferences and policies pointed in a different direction.

1. Hard Structural Constraints

Platforms control a main theater where major modern national security threats and geopolitical dynamics play out. Government actors must rely on platforms to overcome hard constitutional and institutional constraints on their ability to address an expanding category of security and geopolitical challenges.

Constitutional constraints prevent government from taking matters into its own hands. As the law currently stands, the First Amendment likely precludes direct government regulation of content on platforms. Government cannot mandate the removal of content at odds with U.S. national security and foreign relations interests or block users and groups in real time. It cannot dictate related platform policy or directly set platform enforcement priorities.[236] Nor

[236] *See* Reno v. ACLU, 521 U.S. 844 (1997) (striking down the anti-obscenity provisions of Section 230 of the CDA on First Amendment grounds and finding that the special factors the

can government step in and operate on private platform infrastructure to monitor and respond to threats like online influence operations and foreign and domestic terrorism. The Fourth Amendment and existing statutes that allow government to obtain data from platforms limit government's access to the daily intelligence that platforms generate across policy and security challenges.[237]

Institutional constraints similarly force government to rely on platforms substantially in the security and geopolitical space. Platforms created a problem by allowing offline-world security and geopolitical threats like disinformation and violent extremism to thrive and by amplifying them online. But paradoxically, platforms are also the actors best institutionally placed to spearhead efforts to address it. Platforms have the advantages over government of technological expertise, control, and dispatch in their domain. They are on the digital frontlines. They have intimate knowledge of the technological aspects of their own products, services, and infrastructure, their vulnerabilities, and the technical means to overcome them. They constantly monitor user activity and have a deep understanding of online user behavior that government is unlikely to equal even if it throws additional resources and personnel at the problem.[238]

Court had recognized as justifying content-based regulation of the broadcast media are not present in cyberspace); *see also* Klonick, *The New Governors*, *supra* note 18, at 1603-09 (documenting the development of doctrine granting platforms robust First Amendment protection as speakers against government regulation of their content moderation practices); Alan Z. Rozenshtein, *Silicon Valley's Speech: Technology Giants and the Deregulatory First Amendment*, 1 J. FREE SPEECH L. 337 (2021). As we saw in Part III.C, government can impose sanctions on users under the various authorities at its disposal for doing so. Platforms will then need to comply with the sanctions. But imposing sanctions takes time and requires meeting certain procedural and substantive requirements. It is not a good tool for real-time threat management. Furthermore, whether sanctions and the prohibition on providing material support to terrorists require platforms to remove content associated with designated users remains an open question under existing precedent. *See supra* Part III.C.2.ii.

[237] *But see* the discussion of authorities to obtain threat information from platforms, including through the broad authority to issue National Security Letters, in Part III.C.

[238] Platforms could also be said to be better institutionally positioned than government to address certain national security challenges from a substantive point of view, not just because they control the medium where threats manifest or where they are amplified. Take, for example, the controversial area of countering violent extremism (CVE). CVE calls for the prevention of terrorism through community engagement, and it became a component of both global and national counterterrorism efforts against the backdrop of the rise of ISIS. *See, e.g.*, U.N. Secretary-General, *Plan of Action to Prevent Violent Extremism*, U.N. Doc. A/70/674 (Dec. 24, 2016). It attracted criticism across the board. *See, e.g.*, *The Problems with "Violent*

Government-platform institutional disparity in this context also means that a government effort to command platform geopolitical and security practices through traditional regulation is unlikely to be effective, even if there remains a degree of unrealized space to regulate platform security and geopolitical practices within existing constitutional boundaries.[239]

Extremism" and "Violence Prevention" Programs, ACLU, https://perma.cc/KEE8-7XG9; Faiza Patel, Andrew Lindsay & Sophia DenUyl, *Countering Violent Extremism in the Trump Era,* BRENNAN CTR. FOR JUST. (June 15, 2018), https://perma.cc/9WAC-NVQR; Eric Rosand & Stevan Weine, *On CVE, the Trump Administration Could Have Been Worse, but It's Still Not Good Enough*, BROOKINGS INST. (Apr. 7, 2020), https://perma.cc/V9A2-FZXG; Peter Beinart, *Trump Shut Programs to Counter Violent Extremism*, ATLANTIC (Oct. 29, 2018), https://perma.cc/U76X-RFZA.

The Obama administration launched multiple initiatives to "undermine the attraction of extremist movements and ideologies that seek to promote violence" and "address the root causes of extremism through community engagement." CVE efforts extended to foreign actors like al-Qaeda and ISIS, but also to domestic actors propagating violent ideologies. It involved government promotion of "social media solutions"—collaboratively developing "digital content that discredits violent extremist narratives and amplifies positive alternatives." *See Fact Sheet: The White House Summit on Countering Violent Extremism*, WHITE HOUSE (Feb. 18, 2015), https://perma.cc/7T8Z-LJUP.

The Trump administration gutted and largely abandoned these initiatives. *See* sources cited *supra*. They are widely considered a failure, suggesting that large-scale public diplomacy to prevent the spread of violent extremism at the local level is not a task best suited for the federal government. The Obama administration recognized this by harnessing social media companies to participate in creating and amplifying content to counter violent ideologies, while also reaching out to local and religious actors. Platforms are arguably better placed to disseminate such content and to engage in large-scale public diplomacy of this sort than government because of their proximity to users, familiarity with user interests, and degree of control over national and international information flows. In other words, here, too, institutional features of both the federal government and platforms create incentives for government to rely on platforms to address certain national security challenges.

[239] Government has latitude to regulate certain platform functions that implicate national security and foreign affairs but do not involve regulation of content. One form of such potential regulation could impose due diligence requirements on platforms with respect to the national security or geopolitical risk that their products create, along the lines of the FCPA model. *See* sources cited *supra* note 189. The federal government has traditionally been considered to have broad and unique powers in those areas. That perception has resulted in looser applications of doctrines and otherwise limiting constitutional obligations with respect to foreign affairs and national security action. *See, e.g.*, Holder v. Humanitarian L. Project, 561 U.S. 1 (2010) (rejecting a First Amendment challenge to the prohibition on providing material support to a Foreign Terrorist Organization); United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) (using a capacious application of the non-delegation doctrine in foreign relations). *But see* Zivotofsky *ex rel.* Zivotofsky v. Kerry (Zivotofsky II), 576 U.S. 1 (2015); Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury, 686 F.3d 965 (9th Cir. 2012) (modifying evidence disclosure requirements under the Fifth Amendment to protect confidential sources).

Traditional regulation, or command-and-control regulation, mandates specific outcomes through universal rules. Scholars have long argued that this form of regulation falls short in governing complex private sector activities, especially ones that involve the exercise of broad policy discretion.[240] Rigid ex ante rules are insensitive to diversity among private companies or the full range of contingencies that they may face. Furthermore, as Kenneth Bamberger and Deirdre Mulligan put it, regulators "have neither the resources nor the vantage to attain the granular knowledge necessary to combat risk within individual companies . . . . [U]niform, static, approaches to regulation are particularly inapt to contexts characterized by rapid changes in technology and market infrastructure."[241]

Platform security and geopolitical activity is exactly that kind of context. Security and geopolitics are fast-changing, constantly evolving policy areas. It is difficult to predict where, when, and how the next bombing, influence operation, or military coup might take place. Platforms are closer to the (online) scene, have better technological understanding of both online threats and potential technological solutions, and are relatively nimble as compared to government bureaucracies. This is therefore a textbook context that invites a different kind of government role, one that draws inspiration from the "new governance" school of thought about regulation. Among other regulatory techniques, new governance approaches emphasize policy experimentation through iterative and flexible long-term public-private partnerships among multiple stakeholders.[242] Government no longer functions as "a singular source of policy expertise and legal command," but instead assumes the role of a

---

[240] *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 L. & POL'Y 477, 480-82 (2011); Gráinne de Búrca & Joanne Scott, *Introduction: New Governance, Law, and Constitutionalism*, *in* 1 LAW AND NEW GOVERNANCE IN THE EU AND THE US 1 (Gráinne de Búrca & Joanne Scott eds., 2006); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MIN. L. REV. 343, 443 (2004) ("The governance model should thus be understood as an attempt to envision a third way between state-based, top-down regulation and a single-minded reliance on market-based norms; between centralized command-and-control regulation and individual free contract."); Cass R. Sunstein, *Administrative Substance*, 1991 DUKE L.J. 607 (1991).

[241] Bamberger & Mulligan, *supra* note 240, at 480.

[242] *See* sources cited *supra* note 240; *see also* MARTHA MINOW, PARTNERS, NOT RIVALS: PRIVATIZATION AND THE PUBLIC GOOD (2002); Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism,* 98 COLUM. L. REV. 267 (1998).

facilitator and focal point that brings all the relevant players together to develop and implement policy.[243]

Given the constitutional and institutional constraints on government, government is not as well placed as platforms to directly manage platform-enabled threats and geopolitical challenges. Public-private partnerships therefore become essential. Government is compelled to rely on platforms for information and operational access. Government also has incentives to empower platforms through informal cooperation, concrete tips, and threat analysis sharing if it wishes to be effective in online threat monitoring and response within fairly tight constitutional constraints.

To date, scholars and practitioners alike have argued that cooperation among national security agencies, private technology companies and other stakeholders is imperative to address novel cybersecurity threats.[244] Discussing a new NSA public-private Cybersecurity Collaboration Center designed to allow NSA and private companies to share information, NSA's Director of Cybersecurity said that "[w]hat we get from the private sector is we get reach into places that NSA doesn't go."[245] He added that private companies offer the NSA a "sensor net" and that "what they're observing fills in that blank spot that we don't see."[246]

However, discussion of the importance of public-private national security partnerships has so far focused on cybersecurity in the narrow sense, that is, protecting U.S. networks and ensuring the continued functioning of critical infrastructure.[247] Public-private cooperation is just as critical for addressing other kinds of online national security and geopolitical challenges, beyond simply protecting the functional integrity of computer networks. Platforms' involvement is essential for responding to the modern incarnation of an

---

[243] *See* Bamberger & Mulligan, *supra* note 240, at 481-82.

[244] For a recent comprehensive treatment of public-private partnerships in cybersecurity, see Eichensehr, *supra* note 22, at 470 ("Calls to establish public-private partnerships in cybersecurity have become ubiquitous. . . . '[P]artnership' has become the watchword for remedying cybersecurity failures in the United States."). The extensive breach of U.S. government and private networks by Russian intelligence, which originated in SolarWinds—a product supplied by a private company—was yet another reminder of how critical the public-private nexus is for cybersecurity. *See* Christopher Bing et al., *Suspected Chinese Hackers Used SolarWinds Bug to Spy on U.S. Payroll Agency—Sources*, REUTERS (Feb. 2, 2021, 10:43 AM), https://perma.cc/Y5GJ-VLBS.

[245] William Turton, *Hush-Hush NSA Lifts Veil on How Businesses Help Fight Hacks (2)*, BLOOMBERG L. (June 23, 2021, 10:10 AM), https://perma.cc/Y5WF-BRYZ.

[246] *Id.*

[247] *See* Eichensehr, *supra* note 22.

important category of national security and geopolitical threats, and government has no choice but to rely on their cooperation because they control key channels through which threat actors operate.[248] Government is even more dependent on platforms here than in the narrow cybersecurity context because of the added First Amendment restrictions on its freedom of direct action.[249]

2. Bureaucratic Workarounds

There are reasons other than overcoming hard constitutional and institutional constraints that may bring government agencies and individual actors within agency bureaucracies to operate through indirect and informal cooperation with platforms on national security matters. It might sometimes be convenient for government actors to use platforms as bureaucratic workarounds even when government has legal authority and institutional competence to act on its own. Government actors, particularly in the Executive, may use platforms to advance policies and outcomes that would otherwise be more difficult for them to realize because of legal, pragmatic, or political obstacles.[250]

---

[248] *Cf.* Daphna Renan, *Pooling Powers,* 115 COLUM. L. REV. 211, 213-14 (2015) (describing the practice of government agencies pooling their resources and expertise together to address novel threats in order to overcome deficiencies in their individual capacities to address them).

[249] The National Security Commission on Artificial Intelligence Report, produced by a congressionally-nominated bipartisan commission chaired by former Google CEO Eric Schmidt, acknowledged that "[i]n the United States, the private sector has taken the leading role in combating foreign malign information. Social media companies in particular have extensive operations to track and manage information on their platforms. But coordination between the government and the social media firms remains ad hoc. We need a more integrated public-private response to the problem of foreign-generated disinformation." *See* NAT'L SEC. COMM'N ON A.I., FINAL REPORT 48 (2021). The Report recommends that Congress authorize "a Foreign Malign Influence Response Center . . . within the Office of the Director of National Intelligence (ODNI). The government should use this authority to create a technologically advanced, 24-hour task force and operations center to lead and integrate government efforts to counter foreign-sourced malign information. It would survey the landscape of relevant public and private actors, coordinate among them, and act in real time to counter foreign information campaigns." *Id.*

[250] This definition adopts, with modifications, Jon Michaels' definition of privatization workarounds. In his account, "workarounds are government contracts . . . that provide the outsourcing agency with the means of achieving distinct public policy goals more readily than would be possible in the ordinary course of nonprivatized public administration." Jon D. Michaels, *Privatization's Pretensions*, 77 U. CHI. L. REV. 717, 727 (2010). Privatization workarounds allow executive actors to transform policy under the pretext of "technocratic"

Legal obstacles: cut through administrative procedure and circumvent substantive legal requirements. As we saw in Part III.C, platforms are largely unconstrained by constitutional, administrative, and statutory legal obligations that often limit the government's own freedom of action.[251] Such obligations include the First and Fourth Amendment, constitutional due process obligations, the administrative law requirement of fact-based, rational decision making,[252] and substantive and procedural statutory criteria for applying certain measures like economic sanctions or imposing criminal liability for material support for terrorism.[253]

Platforms are also all but immune to judicial review of their content moderation decisions thanks to Section 230 of the CDA.[254] Despite the increased deference government traditionally gets in the areas of foreign affairs and national security, the possibility of judicial review and intervention still lurks in the background—especially when government acts against identifiable individuals and entities.[255]

Therefore, relying on platforms as the governments' long arm has the advantage of allowing national security and public safety agencies to advance certain actions when they prefer not to follow the legal procedures and obligations that would apply to their actions had they acted themselves. This could happen when agencies or individuals within them find legal requirements too cumbersome, when it is doubtful that the situation meets applicable legal criteria such as substantive statutory requirements or procedural and

---

privatization ostensibly designed to provide public goods more efficiently. Paradigm examples in Michaels' account include a national security agency outsourcing a data mining operation for counterterrorism intelligence gathering to a private contractor unconstrained by legal standards that would apply to a similar government operation, entering contracts to perpetuate policies that would bind future administrators, and hiring contractors to augment available military forces and obfuscate casualty numbers. *Id*. at 719-22.

My account of bureaucratic workarounds, by contrast, is not limited to instances of formal outsourcing of government functions via contract. In today's landscape of powerful private actors controlling important aspects of public life, workarounds increasingly occur in informal, flexible, and dynamic settings. They do not necessarily depend on the existence of a formal legal instrument. I return to this point in Part IV.B.

[251] *Cf*. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 255 (2007) (pointing to the gap between federal agency and private sector regulation of the collection and storage of personal information).

[252] Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29 (1983).

[253] *See supra* Part III.C.

[254] *Id.*

[255] *See* Chachko, *supra* note 167, at 1130-36.

evidentiary requirements, or when agencies would like to avoid setting a precedent for future government action. It is much easier to rely instead on platforms exercising their far less regulated policy and enforcement discretion.

Because of the informal and opaque nature of these kinds of interactions and the dearth of reporting about them, it is difficult to point to a concrete U.S. example of government reliance on platforms to cut through legal and procedural requirements. But examples from other jurisdictions are illustrative. The Israeli State Attorney's Office operates a cyber unit whose role is to informally reach out to platforms and request that they remove content that the State judges to be dangerous or unlawful.[256] There is no legislation authorizing this practice. Bureaucrats in the cyber unit and their colleagues could address user behavior they judge problematic through multiple conventional legal routes: obtaining a court order to remove content, initiating a criminal investigation, imposing sanctions on users, or availing themselves of numerous counterterrorism authorities under Israeli law. Instead, the State's Attorney's Office prefers what amounts to picking up the phone and asking relevant platform officials to have content removed.[257] A similar "internet referral unit" exists in the European Union.[258]

Pragmatic policy reasons. Government actors may rely on platforms as bureaucratic workarounds for pragmatic policy reasons. Urgency is one such reason. Warning a platform official about a potential imminent threat could be faster and more effective than mobilizing an unwieldy interagency process to address the threat through government channels. Moreover, government often has reasons to obscure its role in identifying or acting against online threats, such as protecting sources and methods or avoiding an overt standoff with a foreign actor. As Kristen Eichensehr observed in the cybersecurity context, attribution of cyberattacks to foreign actors is an area in which government has sometimes opted to act through private actors instead of publicly attributing attacks itself.[259]

Political obstacles: circumvent internal political opposition. Indirect privatization of government tasks to platforms can be the result of internal tensions within government. It could be a way for the Executive to act in

---

[256] HCJ 7846/19 Adalah v. Israel Office of the State Attorney __ PD __ (Apr. 12, 2021) (Isr.), https://perma.cc/2MUN-P5YZ.

[257] *See id.*

[258] *See EU Internet Referral Unit–EU IRU: Monitoring Terrorism Online*, EUROPOL, https://perma.cc/BT33-AV3R.

[259] *See* Eichensehr, *supra* note 22, at 489-94.

contravention of Congress's stated preferences or to circumvent congressional oversight. And it can serve as an outlet for sidestepping obstacles *within* the executive branch.

As the saying goes, the executive branch is a "they," not an "it."[260] One frequent source of internal friction is disagreement between the civil servants in the administrative bureaucracy and political leadership. Nowhere have these tensions been more apparent of late than in CISA's cooperation with platforms to protect the credibility of the 2020 U.S. election, fight unfounded claims of election fraud, and counter exaggerated rumors about foreign interference. While this was taking place, the Trump White House mounted a political, legal, and media campaign alleging massive voting fraud and asserting that the elections had been "stolen," [261] contrary to the assessment of the administration's own election security experts.[262] The President even fired CISA's head for refusing to align with the White House.[263]

Meanwhile, as Part III.A.2 shows, CISA engaged in close cooperation with platform trust, safety and election integrity officials in the framework of the election integrity working group around goals and insights that aligned with the agency's own assessment—not that of the White House. Although we know little about the content of these frequent exchanges, one could speculate that the forum and the personal working relationships that developed around it became conduits for advancing CISA's threat assessment and enforcement priorities through platforms while trying to avoid overt clashes with the president and his close environment.

Political-bureaucratic tensions about threat assessment and related policy may drive agency experts and career civil servants in the national security space to work with platforms through informal cooperation mechanisms and the cultivation of personal working relationships. Such use of platforms as bureaucratic workarounds allows agencies and actors within them to circumvent political roadblocks and advance goals discouraged or actively

---

[260] *See, e.g.*, Elizabeth Magill & Adrian Vermeule, *Allocating Power Within Agencies*, 120 YALE L.J. 1032, 1036–38 (2011); Eric A. Posner, *Deference to the Executive in the United States After September 11: Congress, the Courts, and the Office of Legal Counsel*, 35 HARV. J. L. & PUB. POL'Y 213, 235 (2012).

[261] Sources cited *supra* note 3.

[262] *See Joint Statement from Elections Infrastructure Government Coordinating Council & The Election Infrastructure Sector Coordinating Executive Committees*, CYBERSEC. & INFRASTRUCTURE SEC. AGENCY (Nov. 12, 2020), https://perma.cc/93R9-G5CF ("The November 3rd election was the most secure in American history.").

[263] Sources cited *supra* note 2.

opposed by political leadership. If you will, it is an avenue for bureaucratic resistance.[264]

3. Platforms as Substitutes

The previous categories involve different versions of collaborative government-platform dynamics. In this final category, platforms act unilaterally to fulfill traditional government national security and geopolitical functions as *substitutes* for government. Platforms do so when their policy preferences contradict government's selected course of action, or when they are required to fill a policy void left by government due to indecision, neglect, or lack of interest.

One example of confrontational substitution is platforms' role in countering domestic violent extremism under the Trump administration. Platforms have taken the lead in developing and enforcing policies against home-grown militarized movements. While the Trump White House tacitly encouraged groups that propagated violence and conspiracy theories, [265] platforms enforced against users and accounts connected to such groups. The QAnon wholesale deplatforming and the aftermath of the January 6 capitol riots are key examples.[266] Another Trump administration example is platforms' effort to combat COVID-19 disinformation even as the administration—including the President himself—avoided action, denied the scope of the crisis, advocated against taking precautions, promoted untested or harmful cures, and propagated unrealistic projections about vaccine development and distribution.[267]

In other cases, platforms have assumed traditional government geopolitical and national security functions by default, due to government inaction or withdrawal from certain policy areas and regions where platforms operate. The absence of a clear United States policy on certain geopolitical and security

---

[264] *Cf.* Jennifer Nou, *Civil Servant Disobedience*, 94 CHI.-KENT L. REV. 349 (2019); Rebecca Ingber, *Bureaucratic Resistance and the National Security State*, 104 IOWA L. REV. 139 (2018). Of course, many would find agencies acting in contravention of political leadership objectionable in most cases. My analysis here is purely descriptive. It does not imply a normative position as to the desirability of such action.

[265] *See, e.g.*, Charlie Savage, *Incitement to Riot? What Trump Told Supporters Before Mob Stormed Capitol,* N.Y. TIMES (Jan. 12, 2021), https://perma.cc/5K36-BCJZ.

[266] Sources cited *supra* note 146.

[267] Sources cited *supra* note 51.

matters has required platforms to act unilaterally without clear government guidance.

Such was the case in the wake of the recent takeover of Afghanistan by the Taliban in the weeks leading up to the U.S. withdrawal from the country. Facebook, Twitter, YouTube, and others were faced with an urgent need to decide whether and to what extent to allow the Taliban to maintain a presence on their platforms as the group was about to become the effective government in Afghanistan.[268] All the while, governments including the United States avoided articulating a clear policy on that question.[269] In other words, platforms had to decide for themselves whether to recognize the Taliban as the legitimate Afghan government, while accounting for the group's longstanding designation as a terrorist organization subject to U.S. economic sanctions.[270]

Platforms' policy decisions were expected to have significant external implications. Recognition of the Taliban would serve a broader legitimating function. It could influence the policies of sovereigns. And it would create facts on the ground. Allowing the Taliban to use official government accounts would perpetuate the perception that the fact of its sovereignty was settled. Ultimately, Facebook, Twitter and YouTube confirmed that they banned the Taliban. Facebook invoked its dangerous organizations policy while avoiding the recognition question.[271] YouTube emphasized that it complies with "all applicable sanctions" as well as its own policies prohibiting incitement to violence.[272]

Other examples are platforms' work to ensure election integrity in other parts of the world and to prevent atrocities and sectarian violence in global hotspots. Previous administrations, both Democratic and Republican, (controversially) prioritized advancing free and fair elections in other

---

[268] *See* Lima, *supra* note 9; Madhok, *supra* note 9; *see also* Casey Newton, *The Platforms' Taliban Dilemma: A Designated Terrorist Organization Rules Afghanistan. Now What*?, PLATFORMER (Aug. 17, 2021), https://perma.cc/P7BT-S4R9.

[269] *See* Lima, *supra* note 9 ("The United States is still 'taking stock' of the situation and whether to recognize Taliban rule.").

[270] *See id.* (quoting Katie Harbath, a former Facebook official: "It feels unique. . . . It feels like it is not a typical situation that there's like a written playbook for how to handle something like this.").

[271] *Id.* ("Facebook does not make decisions about the recognized government in any particular country but instead respects the authority of the international community.").

[272] *See* Madhok, *supra* note 9.

countries.[273] Among many other examples, then-Secretary of State Hillary Clinton famously criticized Russia's 2011 parliamentary elections. Her comments drew the ire of Russia's leadership and complicated the bilateral relationship between the countries for years to come.[274] By contrast, the Trump administration largely remained silent about what was taking place in foreign elections, including in the face of foreign interference by actors such as Russia similar to patterns identified during the 2016 U.S. election.[275] Platforms, meanwhile, took significant steps to address election integrity in foreign countries.

A third example is the ongoing standoff between the Indian government and platforms. Among several flashpoints in recent months, in May 2021, the Indian police raided Twitter's local offices after the platform labeled a ruling party member's tweet "manipulated media." Platform officials complained that the U.S. government failed to take a clear position to support platforms against foreign government deployment of coercive power against them. Facebook's head of counterterrorism and dangerous organizations said at the time that "I understand that many folks want [the U.S.] putting more pressure on tech for a variety of reasons. Fair enough. But there are a host of issues where [the U.S. government] needs to support tech companies to advance U.S. interests and values."[276]

Finally, the Trump administration de-prioritized human rights protection and atrocity prevention,[277] leaving platforms the task of attempting to contain related crises, at least within their domain. This is not to say that platforms have engaged in these efforts out of sheer altruism and concern for human rights, or

---

[273] *See, e.g.*, THOMAS CAROTHERS, CARNEGIE ENDOWMENT FOR INT'L PEACE, U.S. DEMOCRACY PROMOTION DURING AND AFTER BUSH (2007).

[274] Elise Labott, *Clinton Cites 'Serious Concerns' About Russian Elections*, CNN (Dec. 6, 2011, 11:44 PM EST), https://perma.cc/VM4E-C4AF.

[275] *See* MARIAN L. LAWSON & SUSAN B. EPSTEIN, CONG. RSCH. SERV., R44858, DEMOCRACY PROMOTION: AN OBJECTIVE OF U.S. FOREIGN ASSISTANCE 1 (updated 2019) (finding "bipartisan support for the general concept of democracy promotion" across administrations but noting that "President Trump indicat[ed] in various ways . . . that promoting democracy and human rights are not top foreign policy priorities of his Administration").

[276] Brian Fishman (@brianfishman), TWITTER (May 24, 2021, 7:30 PM), https://perma.cc/2DPX-5JQ8.

[277] *See, e.g.*, ELSINA WAINWRIGHT, U.S. STUD. CTR., HUMAN RIGHTS AND THE TRUMP ADMINISTRATION (2018); Stephen Pomper, *Preventing Atrocity in the Age of Trump*, ATLANTIC (Mar. 5, 2018), https://perma.cc/X7LL-WDEQ; Diane Taylor, *Trump Administration Alters and Downplays Human Rights Abuses in Reports*, GUARDIAN (Oct. 21, 2020 5:00 EDT), https://perma.cc/EX6S-4BFU.

that these efforts have been effective. Platforms' actions have undoubtedly been influenced by public and political pressure and the threat of regulation as a result of major past failures in this area.[278] Whatever their motivations, however, platforms have become more engaged in global crises as the government all but ceded the territory.

4. Summary: National Security by Platform Categories

Table 1 summarizes the categories in which informal privatization of national security and geopolitical functions to platforms may occur and the platform-government dynamic that they typically represent. For each category it notes (1) whether the type of privatization covered is structural—that is, driven by constant systemic features—or contingent on government-platform policy alignment and (2) whether it involves platform-government cooperation or platform unilateralism.

Table 1: Summary of National Security by Platform Categories

	GOVERNMENT-PLATFORM COOPERATION	**PLATFORM UNILATERALISM**
STRUCTURAL	**Hard Constraints** Privatization necessary because of hard constitutional restrictions on government and inherent institutional advantages of platforms (access, technological expertise, dispatch)	———
CONTINGENT	**Bureaucratic Workarounds** Government has legal and institutional competence to act directly but elects to act through platforms for political or pragmatic policy reasons (circumvent law and procedure, obscure government role)	**Platforms as Substitutes** Platforms act in defiance of government or enter a government policy void

[278] *See supra* Part II.A.

Privatization due to hard structural constraints on government will probably continue regardless of the degree of political and policy alignment among Congress, the Executive, and platforms. That category of privatization occurs because of a constant feature of the modern national security and geopolitical ecosystem. Government is constitutionally constrained in ways that prevent it from controlling platform security and geopolitical operations, and it is institutionally inferior to platforms in this space.

Privatization as bureaucratic workaround is contingent on government policymakers' commitment to process and their policy preferences, such as whether to use platforms to indirectly attribute influence operations to foreign countries instead of making an official government pronouncement. It is also contingent on the fluctuating alignment among Congress, political leadership, and career agency personnel. Admittedly, though, this category of informal privatization is enabled in part by a structural asymmetry between government and platforms: platforms are relatively nimble and unconstrained by law in the relevant sense,[279] while government is heavily bureaucratic and constrained by procedures and legal requirements that do not apply to platforms. This incentivizes government officials to leverage platforms to take action that would be far more complicated to undertake through official government channels. Of course, as platforms become larger and more bureaucratic, the practical advantages for government in using them as its long arm when it has the competence to act itself diminish.

By contrast, the category of platforms as substitutes is entirely contingent. It shrinks when there is a large degree of overlap between platform policy preferences and those of the administration in power. Under the Trump administration, platform and administration preferences did not align in many important contexts discussed in Part IV.A.3. Platforms therefore acted in defiance of the administration on key security and safety issues and stepped into policy voids that the administration had left on several geopolitical challenges.

The priorities of the Biden administration, by contrast, seem to align much more closely with platforms' revealed priorities to date. For example, the Biden administration has signaled an intention to tackle homegrown violent extremism by ordering law enforcement and intelligence agencies to refocus

[279] That is, when it comes to the geopolitical and security practices described in this paper.

resources on addressing this problem.[280] The policy breaks with the Trump White House's tacit support for certain domestic militarized groups and is consistent with platforms' treatment of such groups thus far. Biden has also reversed his predecessor's approach to COVID-19, among many other key issues. Therefore, clashes between platforms and the Executive on national security and geopolitical matters in which platforms enter a policy void left by the Executive should be less frequent under the Biden administration compared to the Trump administration. This is not to say that they have disappeared, as the India and Afghanistan examples remind us.[281]

The typology proposed here disaggregates national security by platform—the complex emerging government-platform relationship in the realms of geopolitics and national security. It allows for fine-grained analysis of its various aspects. But is this dynamic different than other instances of privatization of government national security tasks to private actors? How does national security by platform inform existing privatization theory? The next Part turns to these questions.

B. National Security by Platform vs. Traditional National Security Privatization

Privatization of key government functions, including national security functions, is obviously not a new phenomenon.[282] National Security and foreign affairs have traditionally been viewed as core government tasks. Many scholars have argued that such quintessential government functions should not be privatized in the first place.[283] But despite the conceptual-theoretical objections to national security and foreign affairs privatization, in practice one can find many instances and areas in which private actors have assumed government

---

[280] Eric Tucker, *Biden Orders Review of Domestic Violent Extremism Threat,* ASSOCIATED PRESS (Jan. 22, 2021), https://perma.cc/JF5S-G3CL.

[281] *See supra* Part IV.A.3.

[282] *See, e.g.*, Craig Konnoth, *Privatization's Preemptive Effects*, 134 HARV. L. REV. 1937 (2021); Jon D. Michaels, *An Enduring, Evolving Separation of Powers*, 115 COLUM. L. REV. 515 (2015); Gillian E. Metzger, *Privatization as Delegation*, 103 COLUM. L. REV. 1367 (2003); Laura A. Dickinson, *Public Law Values in a Privatized World,* 31 YALE J. INT'L L. (2006); Jody Freeman, *Extending Public Law Norms Through Privatization*, 116 HARV. L. REV. 1285 (2003). For a recent collection of normative writing about privatization, see generally THE CAMBRIDGE HANDBOOK OF PRIVATIZATION (Avihay Dorfman & Alon Harel eds., 2021).

[283] *See*, *e.g.*, Eichensehr, *supra* note 22, at 476 and sources cited therein; Freeman, *supra* note 282, at 1300 (referring to foreign policy and national defense as "activities where privatization seems unfathomable").

national security responsibilities and tasks. Much of the scholarship on national security privatization has focused on the military and intelligence spheres.[284] That focus stemmed in part from backlash following the post-9/11 government excesses and the "surveillance-industrial" complex,[285] as well as the Snowden revelations, which concentrated attention on the government's heavy reliance on private intelligence contractors.[286]

Nevertheless, national security by platform—the pattern of informal and at times indirect privatization of major national security and geopolitical functions that this paper documents—is a relatively new variation on traditional national security privatization. It can be distinguished in certain key aspects from paradigmatic instances of national security privatization. It also significantly expands similar but narrower recent trends in counterterrorism and cybersecurity public-private partnerships.

1. Traditional Privatization Conceptions

There is no single account or definition of privatization. But traditional privatization scholarship has generally conceptualized it as active, deliberate government transfer of functions and tasks that government itself used to perform to private actors through a formal arrangement. That formal arrangement could take the form of contract, de-regulation, statute, or some other positive mechanism or governmental act.[287]

The main U.S. government document setting out privatization-related guidelines is the Office of Management and Budget's Circular No. A-76 regarding "performance of commercial activities" by the private sector.[288] The guidelines require government departments and agencies to actively "[i]dentify

---

[284] *See, e.g.*, P. W. SINGER, CORPORATE WARRIORS: THE RISE OF THE PRIVATIZED MILITARY INDUSTRY (2007); Laura A. Dickinson, *Outsourcing Covert Activities*, 5 J. NAT'L SEC. L. & POL'Y 521 (2012); Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801 (2011); Michaels, *Deputizing Homeland Security*, *supra* note 22; Michaels, *All the President's Spies*, *supra* note 22.

[285] *See generally* JAY STANLEY, ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESS AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY (2004).

[286] *See, e.g.*, Zygmunt Bauman et al., *After Snowden: Rethinking the Impact of Surveillance*, 8 INT'L POL. SOCIO. 121 (2014); Norm Ornstein, *Edward Snowden and Booz Allen: How Privatizing Leads to Crony Corruption*, ATLANTIC (June 20, 2013), https://perma.cc/XAU7-83EN.

[287] *See infra* notes 288-298 and accompanying text.

[288] OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, OMB CIRCULAR A-76 REVISED, PERFORMANCE OF COMMERCIAL ACTIVITIES (2003).

all activities performed by government personnel as either commercial or inherently governmental." [289] Inherently governmental activities are to be performed by government personnel, while private actors may be contracted to perform commercial activities through certain procedures.[290] The document reflects a rigid, formal, legalistic approach to privatization that requires a deliberate government decision to privatize and seeks to maintain a core set of "inherently governmental functions" in the hands of government.

Scholars have mostly considered formal and deliberate privatization arrangements as well. For instance, Gillian Metzger conceptualizes privatization as delegation of government power. "Privatization," she recognizes, "can take a variety of forms," including "government withdrawal from a field of activity or from responsibility for providing services, as for example when government disbands a program altogether or sells off state-owned businesses."[291] Metzger focuses on "a different and more common model of privatization: government use of private entities to implement government programs or to provide services to others on the government's behalf."[292] "Rather than constituting government withdrawal," she observes, "this form of privatization is characterized by a *sharing* of authority between public and private."[293]

Jody Freeman similarly invokes formal and deliberate privatization methods and arrangements when discussing the meaning of privatization. Privatization, she maintains, "describes nothing in particular so much as it suggests a host of arrangements."[294] She mostly mentions formal privatization scenarios including the sale of major public enterprises, deregulation, commercialization of government agencies, removal of subsidies, and "contracting out"—"the assumption by private operators of what were formerly exclusively public services."[295] In a recent study of the evolving public-private system in cybersecurity, Kristen Eichensehr observes that "many legal

---

[289] *Id.* at § 4.

[290] *Id.* Despite this relatively clear guidance, however, many arguably "inherently governmental" functions—including national security functions, incarceration and policing—have been privatized notwithstanding Circular A-76; *see also, e.g.*, BRIAN FORST & PETER K. MANNING, THE PRIVATIZATION OF POLICING: TWO VIEWS (1999); Dae-Young Kim, *Prison Privatization: An Empirical Literature Review and Path Forward*, 20 INT'L CRIM. JUST. REV. 1 (2019); David A. Sklansky, *The Private Police*, 46 U.C.L.A. L. REV. 1165 (1998).

[291] Metzger, *supra* note 282, at 1370.

[292] *Id.*

[293] *Id.*

[294] Freeman, *supra* note 282, at 1287 and sources cited therein.

[295] *Id.*

scholars focus on privatization through 'contracting out' of government services to private entities."[296]

The formalistic conception of privatization as active, deliberate reassignment of previously governmental tasks to private actors through formal legal arrangements permeates scholarship about traditional national security privatization as well.[297] For instance, P.W. Singer's "corporate warriors" depicts the rise of a privatized military industry that sells services, personnel, and strategic advice to governments worldwide. This kind of privatization involves formal transactions and contracts. Laura Dickinson's analysis of government outsourcing of covert action similarly discusses privatization of foreign affairs action through "contracting out."[298]

2. Informal National Security Privatization

Modern privatization patterns—particularly the rise of powerful technology companies that exercise equivalents to government powers—have put pressure on the paradigmatic understanding of privatization. Work on privatization and national security has begun to explore new, informal, models that do not fit neatly into the traditional privatization paradigm. Kristen Eichensehr and Jon Michaels' work on cybersecurity and informal public-private counterterrorism partnerships, respectively, are important contributions in this line of scholarship.[299]

Eichensehr describes a government-private system in cybersecurity wherein private actors increasingly perform arguably public cyber defense functions such as identifying network breaches and vulnerabilities, protecting private networks against espionage and intrusion, and attributing attacks to foreign actors.[300] At the same time, government conducts itself like a regular market player on cybersecurity matters such as acquiring vulnerabilities (zero-days) on the black market. She contends that this system challenges what she calls "procedural" aspects of the common understanding of privatization.[301]

---

[296] Eichensehr, *supra* note 22, at 504–505.

[297] SINGER, *supra* note 284.

[298] Dickinson, *supra* note 284, at 521 ("All of this outsourcing tests our commitment *not to contract out* core governmental functions." (emphasis added)).

[299] Eichensehr, *supra* note 22; Michaels, *All the President's Spies*, *supra* note 22.

[300] Eichensehr, *supra* note 22.

[301] *Id.*

According to Eichensehr, the cybersecurity public-private system often lacks a component of active and deliberate delegation or abdication of power by government. Rather, private actors choose what functions they wish to fulfill. Moreover, since many cybersecurity challenges and tasks are novel, some tasks were never performed by the government to begin with. Therefore, it is impossible to identify a point at which privatization, understood as transfer of government functions to a private actor, occurred. Consequently, the common conception of privatization as "contracting out" government tasks via formal legal instrument does not capture the informal nature of the public-private cybersecurity relationship.[302] The absence of a formal anchor to govern these public-private relationships means a large degree of freedom for private actors. It also leaves government little control over what they do and minimal ability to inject public law values into their operations.

Michaels' earlier work explores informal government partnerships in Bush-era counterterrorism. In contrast to the cybersecurity system Eichensehr describes, in Michaels' account government still initiated and set the parameters for the informal relationship with private sector actors, like it does in paradigmatic instances of privatization. Michaels depicts "the Executive's apparent practice of identifying and then courting private actors, persuading, coaxing, and sometimes deceiving them to enter into 'informal' intelligence-gathering partnerships."[303] Yet, these partnerships lacked the hallmarks of formal legal arrangements. They were "orchestrated around handshakes rather than legal formalities."[304] Their purpose was to circumvent legal requirements such as obtaining court orders and subpoenas to obtain terrorism-related information from the private sector.[305]

National security by platform shares similar characteristics with informal cybersecurity and counterterrorism partnerships. It constitutes privatization in the fundamental sense that core traditional government functions—protecting national security and addressing geopolitical challenges—are performed by private actors. But it diverges from traditional conceptions of privatization on key dimensions. Transfer of government functions to platforms is not necessarily deliberate, there is no anchoring legal instrument, and government

---

[302] *Id.* at 507-11.

[303] *See* Michaels, *All the President's Spies*, *supra* note 22, at 904.

[304] *Id.* at 901.

[305] *Id.* at 904.

is not the gatekeeper—it does not define the scope of privatized functions or oversee their performance by private actors.

First, like other instances of informal public-private security relationships, national security by platform is not explicitly anchored in any formal legal arrangement—statutory or contractual. Although Part III.C shows that there is ambient law that shapes and facilitates the platform-government national security and geopolitical relationship, there is no statute or contract that specifically delegates government responsibility for election security, countering foreign influence operations, terrorism, violent extremism, or global atrocity prevention to platforms like Facebook, Twitter, and YouTube. The platform-government relationship around security and geopolitical issues developed gradually yet spontaneously in an ad hoc fashion around certain problems and incidents. It is not a product of a considered, deliberate government decision to transfer its own national security and geopolitical functions to platforms.

Recalling the typology developed in the previous Part, the category of platforms as substitutes does not involve any form of active government delegation. There is clearly no formal delegation or contracting out of powers when government fails to act and platforms step into the resulting void. Nor is there any explicit or deliberate transfer of government functions when platforms counter willful government action. In those cases, government does not want platforms to act, let alone does it empower them to do so. Platforms nonetheless choose to act in defiance of government in furtherance of their own interests, including their reading of public sentiment and the political landscape.

The other two categories—when government faces hard structural constraints and when government agencies and actors use platforms as bureaucratic workarounds—do not involve formal delegation or contracting out of government functions either. Instead, they involve a complex informal dynamic of overlapping or complementary action, or in Metzger's words, "a *sharing* of authority between public and private."[306]

In both categories, government does not give power away or transfer full responsibility for addressing certain national security threats to platforms. It retains its position as policymaker and enforcer and its authority to, say, impose sanctions against suspected terrorists and those involved in influence operations, prosecute them, act against foreign state backers of such

---

[306] Metzger, *supra* note 282, at 1370.

operations, and so on. Yet, for reasons discussed above, government needs to cooperate with platforms as a practical and legal matter or otherwise encourage platforms to act independently in mutually beneficial ways. Collaboration around takedowns of foreign influence operations, platform replication of government designation mechanisms, and what amounts to unilateral platform expansion of government sanctions blacklists are examples of mutually beneficial platform action that builds on parallel government action.[307]

Second, and relatedly, government does not set concrete parameters for many platform security and geopolitical policies and their enforcement, except by providing and preserving the overarching constitutional and statutory framework, explored in Part III.C, that allows platforms to engage in these practices in the first place. Unlike paradigmatic cases of privatization, platforms do not merely execute government policies under government guidance, criteria, and oversight, or provide government with relatively well-defined goods and services. They have broad discretion to develop policy on any security and geopolitical issue they deem important based on their own interests or to avoid engaging with certain issues.

As we saw in the previous Part, it is not even clear that government is able to set the parameters. The rise of platforms and other internet giants has bred new versions of national security and geopolitical problems that government had not dealt with before. Platforms are arguably the actors with greater expertise in identifying and dealing with threat actors that dwell online by virtue of their control of relevant data and infrastructure. This is also another reason why it is difficult to speak of deliberate transfer of powers and functions from government to private actors in this context—there was no point in time in which government was the sole actor in play.

One implication of this is that platforms' engagement with geopolitics and security is almost entirely voluntary, and so is their related interaction with government. Although platforms are subject to certain legal requirements mandating cooperation with law enforcement,[308] significant elements of platforms' current national security and geopolitical cooperation with government—such as acting on government tips, sharing information, and

---

[307] This is not to say that platform action in this context would always be welcomed by government. The deplatforming of QAnon, for instance, likely did not enjoy the support of the Trump White House.

[308] *See supra* Part III.C.2.

reporting users—are not compelled by government, but rather are driven by business imperatives or fear of theoretical government sanctions. Cooperative government-platform mechanisms that have emerged to tackle election integrity, foreign influence, and terrorism have been entirely voluntary as well. Platforms certainly act voluntarily and independently of government when they function as substitutes for government in the national security and geopolitical space. While platform officials have expressed their desire to institutionalize certain aspects of their security cooperation with government in the area of election integrity, they also have highlighted the advantages of maintaining an informal, voluntary cooperation mechanism like the current one in order to promote maximal buy-in from all relevant stakeholders.[309]

The term "voluntary" here may obscure the role of government threats in nudging platforms to step up their contribution to national security, lest they face unwanted adverse regulation. Platforms, like other private actors, are sensitive to what some have termed jawboning—government pressure on private actors to act a certain way that is not necessarily backed by concrete legal sanctions.[310] Multiple congressional hearings hauling platform officials before congressional committees,[311] constant talk of reforming Section 230 of the CDA, and informal agency pressure on platforms to cooperate on national security and geopolitical matters could have similar effects to binding legal obligations. I do not deny that these tactics motivate platform action. I simply contrast the informal system of national security by platform with paradigmatic patterns of privatization. The latter are typically structured and anchored in a formal *legal* arrangement.

3. New Features

The previous Part highlighted the similarities between national security by platform and earlier instances of informal national security privatization discussed previously. But it also has new and unique features: the absence of

---

[309] *See* Stanford 2020 Election Panel, *supra* note 97.

[310] *See* Bambauer, *supra* note 50.

[311] *See, e.g.*, *Breaking the News: Censorship, Suppression, and the 2020 Election: Hearing Before the S. Comm. On the Judiciary*, 116th Cong. (2020) (statement of Mark Zuckerberg, Chief Exec. Officer, Facebook, Inc.); *Id.* (statement of Jack Dorsey, Chief Exec. Officer, Twitter, Inc.); *Open Hearing on Foreign Influence Operations' Use of Social Media Platforms (Company Witnesses) Before the S. Select Comm. on Intell.*, 115th Cong. (2018).

subject matter or geographic restrictions on the scope of privatized functions and the breadth of policy discretion that private actors exercise.

National security by platform significantly expands informal national security privatization beyond counterterrorism and cybersecurity in the narrow sense of securing computer infrastructure. Major platforms (private actors) have assumed a critical role—sometimes in cooperation with government, sometimes in defiance of government, and other times by supplanting government—in addressing the full spectrum of security and geopolitical challenges facing government today.

The breadth of security, geopolitical policy, and execution discretion that platforms currently exercise is striking. Questions such as what to do about genocide in Myanmar, what kinds of coordinated behavior constitutes security threats and require enforcement, what foreign government blowback might ensue following such enforcement, what is necessary to secure the Indian election and protect its integrity, how to respond to Turkish demands to silence opposition,[312] or what constitutes credible information about COVID-19 are complex and open-ended. They require far broader and more diverse expertise and greater exercise of policy discretion than identifying individual terrorism suspects or monitoring violent groups, finding breaches of computer systems, exposing zero-day vulnerabilities, or even attributing computer breaches to perpetrators.

In other words, previous instances of informal national security privatization involved relatively well-delineated tasks and well-defined subject matter or had dominant technical dimensions. Today, platforms exercise security and geopolitical discretion and enforcement at an entirely different scale, often without any meaningful government guidance (or, for that matter, appropriate platform expertise and resource allocation).

Furthermore, as this paper shows, national security by platform is highly contingent and dynamic, especially in the third category (platforms as substitutes). Its scope ebbs and flows depending on platforms' objectives and priorities—determined in large part by their business interests—and the national security and foreign policy priorities of a given congress and administration. This feature distinguishes it from previously documented informal privatization of counterterrorism or cybersecurity. Both policy areas

---

[312] *See* Jack Gillum & Justin Elliott, *Sheryl Sandberg and Top Facebook Execs Silenced an Enemy of Turkey to Prevent a Hit to the Company's Business*, PROPUBLICA (Feb. 24, 2021, 5 AM EST), https://perma.cc/8K67-6M93.

have been and are likely to continue to be prioritized regardless of political shifts.

The transition from the Trump to the Biden administration illustrates the dynamism of national security by platform. After 2016, platforms assumed an outsized role in addressing national security and geopolitical challenges traditionally addressed primarily by government due in significant part to unique features of the Trump administration, and its specific policies on election integrity, domestic violent extremism, human rights and atrocity prevention, and the COVID-19 pandemic. The broad scope of national security by platform under President Trump was in part a result of government abdication, malpractice, and internal tensions between political leadership and the national security bureaucracy. An administration that restores government leadership on all these challenges would reduce the onus on platforms to act as substitutes for government. As previously mentioned, the Biden administration's policies have so far aligned better with platforms' revealed policy preferences. As a result, government-platform friction on national security and geopolitics has diminished, even as the administration signaled its intent to advance measures adverse to platform interests.[313]

A key exception is the category of cases in which platforms are essential for addressing national security threats due to hard structural constraints on government in controlling and monitoring private networks. National security by platform in this category is similar to informal privatization in counterterrorism and cybersecurity. Any administration will be forced to rely on platforms to address threats that manifest in their products. Public-private cooperation in that area is inevitable regardless of a given administration's policy priorities.

V. GOVERNING NATIONAL SECURITY BY PLATFORM

The previous Part developed a theoretical framework for analyzing national security by platform and explained how it deviates from the established privatization paradigm. This Part turns to preliminary implications for managing this government-platform geopolitical and security relationship. The platform governance and regulation debate has so far been dominated by speech, competition, and privacy concerns. Applying a security lens to the problem

---

[313] *See, e.g.*, Lauren Feiner, *Biden is Loading Up His Administration with Big Tech's Most Prominent Critics*, CNBC (Mar. 9, 2021, 9:48 AM EST), https://perma.cc/EH8U-DSAM.

highlights considerations that may be in tension with these concerns. It focuses attention on the government-platform nexus.

Part IV illustrates that national security by platform in fact consists of three distinct privatization modes, each with unique characteristics. Regulatory interventions should be tailored to each category. In what follows, I consider ways to mitigate some of the harmful implications of national security by platform while leveraging its advantages. The analysis suggests that "soft" institutional arrangements might be an effective second-best approach in the category of hard structural constraints on direct government management of platform security and geopolitical functions. The category of bureaucratic workarounds calls for greater constraints on *government* reliance on platforms to eschew oversight or procedural and legal requirements that apply to government actors. The category of platforms as substitutes raises a different question: should the federal government be able to undercut platform action when it interferes with U.S. security or geopolitical interests, as the doctrine of foreign affairs preemption allows it to do with conflicting state action?

A. Hard Structural Constraints – Soft Cooperative Arrangements

The features of the category of hard structural constraints invite soft, flexible arrangements to govern government-platform cooperation. Scholars and practitioners have criticized burgeoning institutionalized long-term cooperative government-platform mechanisms such as the election integrity working group and the GIFCT.[314] They have warned that such mechanisms could form "content cartels", allowing one actor—platform or government—to decide for the entire online ecosystem what content should be allowed and what content should be banned.[315] However, informal "soft" cooperative arrangements have important advantages in this category, freedom of expression concerns notwithstanding. They offer an alternative to binding traditional regulation that could help inject public law values into platform decision-making. They are also a way for both government and platforms to compensate for their respective institutional weaknesses in addressing online security and geopolitical challenges.

---

[314] *See supra* Part III.A.

[315] *See* Douek, *supra* note 153. Douek advocates increased transparency about these cooperative arrangements; *see also* Danielle K. Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018).

First, an alternative to government coercion through binding regulation is necessary because binding regulation would be an uphill battle. Although Congress and especially the Executive are often assumed to have broad and exceptional powers when they seek to advance foreign affairs and national security interest,[316] the First Amendment is a significant constitutional hurdle for regulating core platform security and geopolitical practices like writing and executing content policy.[317] Existing judicial interpretations of the scope of the First Amendment grant platforms a powerful defense against direct government intervention in content moderation.[318] As Part IV.A.1 shows, even if the constitutional obstacle proves surmountable, new governance approaches to regulation prescribe precisely this form of cooperative, flexible governance mechanisms for private actor conduct that involves large degrees of policy discretion and uncertainty.

Adding to constitutional obstacles, the government-platform geopolitical and security relationship here is not governed by contract. This deprives government of another legal avenue for shaping platform behavior that is often available in other instances of national security privatization.[319]

Second, soft and flexible arrangements institutionalize all but inevitable government-platform cooperation in this category due to deep mutual operational dependence. From the government's point of view, some degree of cooperation with platforms is necessary in a world in which private actors control the theaters where major national security threats play out. Government has inferior expertise and technological capacity in those theaters as compared to platforms. It cannot step in and operate directly on platform infrastructure.[320] This makes government dependent on platforms in this context.

---

[316] *See* sources cited *supra* note 239; *see also, e.g.*, Ganesh Sitaraman & Ingrid Wuerth, *The Normalization of Foreign Relations Law*, 128 HARV. L. REV. 1897, 1900 (2015) ("The defining feature of foreign relations law is that it is distinct from domestic law. . . . In other words, foreign relations is exceptional.").

[317] Congress likely has the power to introduce new law to shape certain aspects of national security by platform along the lines of CFIUS, FCPA, FISA or SCA. It could theoretically prohibit platforms from engaging in certain activities that intersect with national security or regulate private actor intelligence gathering or other aspects of platform security and geopolitical functions. But core elements of national security by platform are protected under current interpretations of the First Amendment. *See supra* Part III.C.1.

[318] *Supra* note 236 and accompanying text.

[319] *See supra* Part III.B.

[320] *See supra* Part III.A.1.

Platforms, for their part, need government assistance to help them overcome expertise and experience gaps in their own capacity to meet a broad spectrum of geopolitical and security challenges. Platforms are only beginning to venture into the world of geopolitical intelligence and threat analysis. They lack government's institutional memory and decades of accumulated tradecraft. Government can illuminate platform blind spots about the offline world and give them a certain degree of political cover. Cultivating government relationships could also prove beneficial for platform interests beyond security and geopolitics.[321]

If certain elements of platform-government cooperation around security and geopolitics are inevitable, and binding regulation would face significant constitutional and practical obstacles, informal institutions become attractive as a second-best alternative for managing this government-platform relationship. From a national security standpoint, they facilitate coordination and help bridge government-platform capacity gaps. They give both sides visibility into the other's actions and decision-making. Moreover, informal arrangements encourage buy-in from platforms and other relevant stakeholders because they provoke less opposition than binding regulation.[322]

Soft and flexible institutions also have normative advantages. They may facilitate gradual norm development around online security management. In the long run they may even help build consensus around binding regulation within existing constitutional boundaries.[323] Moreover, informal cooperative arrangements provide government with a mechanism for injecting public interests and public law values into platform decision-making.

Jody Freeman uses the term "publicization" to describe the process of expanding government's reach into private realms.[324] That process occurs when private actors commit themselves to public goals in return for accessing opportunities to provide services or deliver goods in lieu of the government. The vehicles for imposing public law obligations could be budgeting, regulation,

---

[321] *See supra* Part IV.D.

[322] *See, e.g.*, Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421, 423 (2000) (arguing soft governance mechanisms provide "certain benefits not available under hard legalization. [They] offer[] more effective ways to deal with uncertainty" and "[facilitate] compromise, and thus mutually beneficial cooperation, between actors with different interests and values, different time horizons and discount rates, and different degrees of power.").

[323] *Id.*

[324] *See* Freeman, *supra* note 282, at 1285.

or contract. Informal institutional arrangements give government actors a vehicle for "publicizing" platform security and geopolitical practices despite the absence of standard mechanisms like contracts or budgetary control that exist in traditional privatization contexts. For instance, government actors can condition security and geopolitical information sharing on platforms subscribing to principles of procedural fairness and privacy when they target users or networks on security or geopolitical grounds. Over time, they can influence platform priorities and policies to align them with U.S. national security and geopolitical interests.

In sum, the features of the category of hard structural constraints make soft cooperative arrangements an appealing second-best approach for managing this aspect of national security by platform. If structural factors mandate platform-government national security and geopolitical cooperation, there is value in creating institutions for managing it compared to the alternative of haphazard interactions.

There are important caveats. The normative value of such arrangements hinges on the degree to which government actors operate in good faith, in compliance with applicable law, and with the public interest and individual liberties in mind. Government conduct in relation to platforms may fall short of that ideal, as recent experience under the Trump administration demonstrates.[325] Platforms amplify restrictive government national security practices like blacklisting and surveillance. Institutionalizing cooperation would entrench this dynamic further.

Still, the risk of government abuse of informal cooperative arrangements with platforms is not unique to this context. This caveat applies to any aspect of government action. It is especially true for government conduct in national security and foreign affairs, which is subject to less stringent constraints and is far less transparent than other areas of government action. The question is not whether soft informal arrangements are ideal. They are not, as they may facilitate a variety of abuses. The question is whether they are preferable to ad hoc government-platform cooperation.

B. Streamlining Bureaucratic Workarounds

The category of bureaucratic workarounds covers instances in which government actors have legal and institutional competence to act but choose

---

[325] *See, e.g.*, sources cited *supra* note 3.

to work through platforms for internal political or pragmatic reasons.[326] Some of those reasons—like urgency or a need to obscure government's role to protect sources or avoid international conflict—are arguably benign. Others, like attempting to accomplish something through platforms without meeting legal and procedural requirements that apply to government actors or circumventing opposition from other government actors, may not be.

In both cases, this practice raises concerns. It is undocumented, secret, and haphazard. Reliance on platforms as bureaucratic workarounds where government has the capacity to act directly replaces somewhat constrained government actors with largely unconstrained private ones.[327] It may therefore undermine congressional and what little judicial oversight exists in foreign affairs and national security. Direct oversight of platform security and geopolitical operations is at present minimal. Part III.C shows that platform security and geopolitical action is all but immune to judicial review. Congress may bring tech platform officials in to testify before its committees, as it has often done.[328] It can address big picture platform regulation issues within constitutional boundaries. But Congress lacks the tools, bandwidth, or political incentives to oversee the minutiae of daily platform security and geopolitical policy development and enforcement. It cannot influence those activities through appropriations as it does with respect to national security and foreign affairs activities of government agencies.[329]

Another concern in the category of bureaucratic workarounds is the use of platforms to flout ordinary government processes and substantive legal requirements that apply to government action. As Part II shows, platforms take cues and accept intelligence from government actors regarding where to search for deceptive or otherwise harmful behavior and against whom to enforce. It would not be a stretch to speculate that government actors might encourage platforms to engage in heightened monitoring or impose unilateral restrictions against certain individuals and groups that they cannot or will not indict or

---

[326] *See supra* Part III.A.2.

[327] *Id.*; *see also* Michaels, *supra* note 250.

[328] *Supra* note 311.

[329] *Cf.* Rebecca Ingber, *Congressional Administration of Foreign Affairs*, 106 VA. L. REV. 395 (2020) (discussing the limits of congressional oversight over government national security and foreign affairs action).

sanction through formal legal channels.[330] In those scenarios, platforms effectively act as the Executive's long arm.

Regulatory interventions should therefore begin with tightening constraints on *government* actor reliance on platforms to advance security and geopolitical goals through bureaucratic workarounds. This is low-hanging fruit because Congress and certainly the Executive have authority and capacity to streamline this process and increase oversight to protect against abuses. The constitutional obstacles that exist with respect to platform regulation are not a factor here. Several preliminary directions for accomplishing this are worth considering.

One category of interventions may be aimed at increasing internal government transparency with respect to this practice. Agencies may require that their officials document and periodically report to agency leadership informal requests and intelligence tips shared with platforms.[331] Congress may require such reporting through legislation. It would be difficult for the Executive to credibly object to the sharing of information with Congress that it was willing to share with private actors on state secrets or executive privilege grounds. Although transparency has limits and may impose policy costs without really facilitating robust oversight,[332] limited reporting requirements should not be particularly onerous. In addition to enabling some internal oversight, these

---

[330] Of course, platforms might also be a constraining force on government blacklisting practices by scrutinizing government "tips" and pushing back against government requests in this context. Available information does not allow us to rule this out. Since platform-government cooperation mechanisms are shrouded in secrecy and lack transparency, it is difficult to evaluate the substance of their interactions. More information about the nature and content of government-platform exchanges is necessary to fully assess their potential advantages and downsides. That being said, recent experience provides reasons to doubt that platforms engage in meaningful scrutiny of government blacklisting practices. In certain areas, in particular threats to election integrity and terrorism, the current posture of Facebook and Twitter, at least, appears to be highly cooperative with government. *See* sources cited *supra* note 2; Wright, *supra* note 184.

[331] Platforms release data about government requests, but these data only cover requests for data pursuant to judicial subpoena or warrant and various legal authorities, including FISA, and national security letters. They do not cover informal intelligence tips that government provides to platforms or other elements of operational government-platform cooperation. *See, e.g.*, *United States*, FACEBOOK TRANSPARENCY CTR., https://perma.cc/3KN2-WUUC.

[332] *See* David E. Pozen, *Transparency's Ideological Drift*, 128 YALE L.J. 100 (2018) (arguing that transparency can be used as a weapon and can have negative policy costs).

interventions could deter use of platforms to circumvent procedure and law that applies to government absent a compelling policy rationale.[333]

Another technique may be for agencies with security or foreign relations missions that interact with platforms to issue guidance that would clarify the circumstances in which agency actors may operate through platforms. Such guidance could outline legitimate policy reasons for government actors to use platforms as their long arm instead of acting directly, such as the need for an urgent response, protection of government sources and methods, or concealment of the government's role in order to avoid overt confrontation with a foreign country.

This is easier said than done. It is hard to clearly distinguish compelling policy reasons from instances in which government players only seek to end-run applicable law and procedure. It would be harder still to prevent reliance on platforms to circumvent internal political opposition to a certain policy course. The aim of the discussion here is not to outline a concrete roadmap for such guidance. Rather, the aim is to point to the need for structuring government actors' discretion in using platforms as bureaucratic workarounds.

C. Platform Preemption?

Unlike the previous two categories, the category of platforms as substitutes does not involve government-platform cooperation. Platforms act unilaterally, and they either defy government or step into a policy void. The latter case is not inherently problematic from a governance standpoint. For better or worse, private actors operate in geopolitical and security contexts all the time.[334] The former case, however, raises a complex question: is there room to constrain platform geopolitical and security action when it clashes with explicit government foreign or security policy? If platforms are increasingly stepping into government's shoes in the foreign and security arena, and if their scale of operations renders their influence comparable to sovereigns, should they be aligned with U.S. national foreign and security policy? Or should policy pluralism in this space be encouraged?

The question invites comparison to familiar doctrine that allows the federal government to undercut competing actions by other actors in the foreign affairs

---

[333] It is possible, of course, that something like this reporting requirements already exists within the Executive. If it does, bringing its specifics to light would be a step forward by allowing scrutiny by outside observers.

[334] *See* sources cited *supra* note 38.

and national security realms.[335] Courts have invoked the doctrine of foreign affairs preemption to strike down state measures that contradicted federal foreign relations statutes, [336] treaties, and international executive agreements.[337] The Supreme Court even preempted state action that touched on foreign affairs in the absence of controlling positive federal law.[338]

Underlying the various strands of the foreign affairs preemption doctrine is the notion that "foreign policy attitudes" are "of course . . . matters for the Federal Government,"[339] and that the nation should be "one as to all foreign concerns."[340] The Supreme Court has invoked a diversity of justifications for this doctrine. One line of justification focuses on preserving the federal governments' foreign relations prerogatives.[341] Another line of justification invokes functional considerations, such as preventing international conflict or confusion about United States foreign policy among foreign nations.

Full consideration of the applicability of the preemption rationale to the government-platform relationship exceeds the scope of this paper. But it is clear that existing judicial justifications for the doctrine in the federalism context are not translatable to the government-platform relationship. Platforms are not states. They are not sovereigns, and they are not a part of the U.S. federal system. They are global companies. They do not speak for the

---

[335] *See*, *e,g.*, Michael D. Ramsey, *The Power of the States in Foreign Affairs: The Original Understanding of Foreign Policy Federalism*, 75 NOTRE DAME L. REV. 341 (1999); Peter J. Spiro, *Foreign Relations Federalism*, 70 U. COLO. L. REV. 1223 (1999); Brannon P. Denning & Jack H. McCall Jr., *The Constitutionality of State and Local Sanctions against Foreign Countries: Affairs State, States Affairs, or a Sorry State of Affairs*, 26 HASTINGS CONST. L.Q. 307 (1998); Jack L. Goldsmith, *Federal Courts, Foreign Affairs, and Federalism*, 83 VA. L. REV. 1617 (1997).

[336] Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363 (2000); Hines v. Davidowitz, 312 U.S. 52 (1941); *see also* Jack L. Goldsmith, *Statutory Foreign Affairs Preemption*, 2000 SUP. CT. REV. 175 (2000).

[337] Am. Ins. Ass'n v. Garamendi, 539 U.S. 396 (2003); Clark v. Allen, 331 U.S. 503 (1947).

[338] Zschernig v. Miller, 389 U.S. 429 (1968); *see also* Carlos Manuel Vazquez, *W(h)ither* Zschernig*?*, 46 VILL. L. REV. 1259 (2001).

[339] Zschernig, 389 U.S. at 437–38.

[340] Letter from Thomas Jefferson to George Washington (Aug. 14, 1787), *in* THE DIPLOMATIC CORRESPONDENCE OF THE UNITED STATES OF AMERICA FROM THE DEFINITIVE TREATY OF PEACE, 10TH SEPTEMBER, 1783, TO THE ADOPTION OF THE CONSTITUTION, MARCH 4, 1789 78 (U.S. Dep't State, ed., Washington, Blair & Rives 1837); *see also* Jean Galbraith, *Cooperative and Uncooperative Foreign Affairs Federalism*, 130 HARV. L. REV. 2131 (2017) (reviewing MICHAEL J. GLENNON & ROBERT D. SLOANE, FOREIGN AFFAIRS FEDERALISM: THE MYTH OF NATIONAL EXCLUSIVITY (2016)).

[341] *See* Goldsmith, *supra* note 335, at 1630.

United States, and—unlike states—their pronouncements on geopolitical and security matters cannot be imputed to the United States.

Moreover, there are good reasons to preserve government-platform policy pluralism. Major platforms can (in principle, if not in practice) leverage their power and social influence to serve as a check against government abuse, negligence, and excess. Platforms have done so in several contexts in the past. To cite a recent set of examples, platforms' actions on COVID-19 and domestic violent extremism helped offset negligent or harmful government action. As we saw in Part I, platforms have acted to counter COVID-19 disinformation and worked to highlight credible sources about issues related to the pandemic. Likewise, when the Trump White House fanned domestic violent extremism and avoided meaningful steps to prevent resulting violence, platforms helped contain violent groups by acting against QAnon, the Proud Boys, and other militarized movements, and eventually deplatforming the President himself for inciting the capitol riots.[342]

D. Capture

The previous Parts focused on potential regulatory interventions in each category of national security by platform. Before concluding, one last observation is in order about the impact on platform regulation of national security by platform as a whole. The government-platform mutual dependence in national security and geopolitics makes it likely that national security by platform will endure even in the shadow of clashes between government and platforms concerning other aspects of their activities. Despite recent high-profile government efforts to take on platforms by stripping or limiting their Section 230 liability protections and initiating antitrust action,[343] both platforms and government have strong incentives to preserve a cooperative relationship on issues such as disinformation, foreign influence operations, election integrity, and foreign and domestic terrorism.

---

[342] *Supra* note 3.

[343] *See, e.g.*, Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Cong. (2021); Press Release, Fed. Trade Comm'n, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), https://perma.cc/EB5Z-563X; Press Release, U.S. Dep't of Just., Justice Department Sues Monopolist Google For Violating Antitrust Laws (Oct. 20, 2020), https://perma.cc/92Z3-T8LK; Press Release, Fed. Trade Comm'n, FTC to Examine Past Acquisitions by Large Technology Companies (Feb. 11, 2020), https://perma.cc/AQ2B-UEDT.

Furthermore, many experts and policymakers have argued that the size and market power of major platforms like Facebook, Google, and Amazon are unsustainable and that it is necessary to break them up or to prevent them from acquiring new companies.[344] But from a national security vantage point, platform size and the dominance of several major players might be an advantage. The fewer players involved in policing and responding to online threats, the easier it is for government to build partnerships and coordinate public-private responses to geopolitical and security challenges.

In other words, policymakers will have to balance competition and speech interests with national security interests in devising platform regulation. Those interests do not point in the same direction. National security regulators may want to avoid action that would diminish major players' market power or their ability to address national security and geopolitical threats within their domain. Their relationships with platform officials in the trust and safety space and the revolving door between government and platform in those areas create a risk of regulatory capture. If the past is any indication, national security agencies are a powerful government constituency. This may complicate efforts to promote regulation adverse to platform interests to advance other societal goals, such as ensuring the free flow of information, protecting user privacy, and increasing competition.

VI. CONCLUSION

Platforms' geopolitical turn and their evolving relationship with government around security and geopolitical issues is an emerging component of the new world of post-2016 platform governance. This paper analyzed the government-platform nexus in these areas as an instance of national security privatization and situated it in the broader context of privatization theory. National security by platform is a complex, part cooperative, part adversarial public-private relationship. Some of its elements are likely to endure even as government clashes with platforms on other fronts. Others are contingent on the identity and policies of a given administration and the extent to which they align with government priorities. Studying and evaluating these dynamics is crucial for understanding the modern national security ecosystem and the role of law and institutions therein. The paper lays a foundation for that discussion.

---

[344] *See* sources cited *supra* note 343; *see also, e.g.*, Khan, *Separation of Platforms*, *supr*a note 18; Khan, *Amazon's Antitrust Paradox*, *supr*a note 18; *Break Up Big Tech*, WARREN, https://perma.cc/AR7S-J3ZF.