AMERICAN Affairs

June 2026 Special Symposium

Securing the Digital Republic:

A Symposium on Cybersecurity

Justin Sherman and Gavin Wilde

Emerson T. Brooking

Joshua Steinman

Lars Erik Schönander, Joshua Levine, and Adam Gluck

Haiman Wong

Matt Stoller

AMERICAN Affairs

June 2026 | A Symposium on Cybersecurity

CONTENTS

Editors' Introduction: Securing the Digital Republic 4

Data-Broke: U.S. Tech Firms' Counterintelligence Dilemma
by Justin Sherman and Gavin Wilde 6

Exploitable by Design: Social Media and the AdTech Threat
by Emerson Brooking 17

The Factory Floor Is Now the Battlefield
by Joshua Steinman 30

How to Safeguard America's Critical Infrastructure
by Lars Erik Schönander, Joshua Levine, and Adam Gluck 32

"I've Been Scammed, Now What?": The Growing Crisis Facing Everyday Americans
by Haimain Wong 40

Tyrants of the Algorithm: Big Tech's Corrosive Rule and Its Consequences
by Matt Stoller 54

AMERICAN Affairs

June 2026 | A Symposium on Cybersecurity

EDITOR	Julius Krein
DEPUTY EDITOR	Gladden Pappin
EXECUTIVE EDITOR	Daniel Bring
ENERGY EDITOR	Travis Kavulla
NATIONAL SECURITY EDITOR	Alexander Alden
SENIOR EDITOR	Michael Cuenco
ASSOCIATE EDITOR	Nicholas Podell
EDITORIAL FELLOW	Samuel Spound

CONTRIBUTING EDITORS

David Adler • Jasper Boers • Oren Cass • David P. Goldman
Joel Kotkin • Malcom Kyeyune • Michael Lind • James Poulos

American Affairs is published quarterly by American Affairs Foundation Inc., One Boston Place, Suite 2600, Boston, Massachusetts 02108, a nonprofit corporation organized under section 501(c)(3) of the Internal Revenue Code.

Price: $12 per copy (USA), $16 (Canada). Print plus digital subscriptions: $36 for one year. For Canada, add $12 per year. For all other international subscriptions, add $24 per year. Digital only subscriptions: $24 per year. Postmaster and subscribers: send change of address, all remittances, and subscription inquiries to *American Affairs*, P.O. Box 3000, Denville, New Jersey 07834. Notice of nonreceipt must be sent to this address within three months of the issue date. Nonprofit postage paid at Boston, Massachusetts, and additional mailing offices.

ISSN 2475-8809

Opinions expressed in articles herein, whether signed or unsigned, do not necessarily represent the views of the editors, board of advisers, American Affairs Foundation Inc., or its board of directors. Nothing in this journal is an attempt to influence the passage of any legislation or the election of any candidate.

All contents Copyright © 2026 by American Affairs Foundation Inc., unless otherwise noted.

SUBSCRIPTIONS: *telephone* +1 (855) 280-1207 *email* custsvc_amaffair@fulcoinc.com
LETTERS TO THE EDITOR: *email* letters@americanaffairsjournal.org
GENERAL INQUIRIES: *email* info@americanaffairsjournal.org

Editors' Introduction: Securing the Digital Republic

Cybersecurity has emerged as one of the defining policy challenges of the twenty-first century. From ransomware attacks on businesses and schools to hacks into our critical infrastructure, from virtual political influence operations to large-scale fraud and nefarious data collection by corporations and state actors, cybersecurity has become an indelible concern of contemporary life.

Adversarial states view cyberspace as an arena for strategic competition below the threshold of conventional warfare. China's formidable espionage capabilities have been successfully directed at governments and businesses alike; Iranian malware has compromised critical American infrastructure; Russia's attacks on the Ukrainian grid have demonstrated that cyber operations can augment hard power on the battlefield.

Simultaneously, advances in artificial intelligence have dramatically accelerated the scale and complexity of cybercrime, lowering barriers for attacks while increasing pressure on government and industry to invest in burdensome protections absent a federally coordinated strategy.

Despite these swelling challenges, many of the United States' digital vulnerabilities are still gaping. Our critical infrastructure functions on half-century-old industrial systems that were not designed for a lawless and hostile cyber environment. Economic incentives encourage the collection and monetization of personal data despite the magnitude of associated risks. Americans face an increasingly sophisticated ecosystem of fraud that exploits technological openness faster than our political institutions can respond. Each of these emergencies compels us to ask whether our digital infrastructure is governed in the public interest or by exploitable commercial incentives misaligned with the common good.

The essays in this symposium examine these interconnected challenges from a range of complementary perspectives, exploring both the sources of the United States' growing digital vulnerabilities and the policy choices available to address them.

In a world of overabundant information, national security threats are discovered by Justin Sherman and Gavin Wilde at the intersection of data collection and counterintelligence. Emerson T. Brooking examines foreign influence on social media platforms, finding gaping legislative inadequacies in the protection of our national discourse. Amid a vastly more complex threat environment, Joshua Steinman makes the case for heightened security and vigilance at America's industrial firms. Lars Erik Schönander, Joshua Levine, and Adam Gluck forecast the mounting cybersecurity risks facing America's critical infrastructure, arguing that operational technology systems have become vulnerable to state-backed campaigns assisted by advanced AI. Haiman Wong addresses the lucrative industry of global fraud and online scams relentlessly targeting ordinary Americans. Lastly, Matt Stoller reviews Sarah Wynn-Williams's *Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism* (Flatiron Books, 2025), using the memoir as a lens through which to examine the evolution of Meta and the political economy of Big Tech.

Taken together, these essays reveal that cybersecurity is no longer a question of defending corporate networks from hackers or maintaining counterintelligence procedures. It has grown to encompass the basic protection of our society at large. Ensuring our digital systems do not endanger but serve the public interest will require new approaches that bridge cybersecurity, economic policy, and national security. We hope the essays collected here contribute to a more complete understanding of the policy choices that lie ahead.

– The Editors

Data-Broke: U.S. Tech Firms' Counterintelligence Dilemma

by Justin Sherman and Gavin Wilde

Nearly a decade has passed since the breach of the U.S. Office of Personnel Management (OPM) by Chinese state-backed hackers in the spring of 2015. That the operation netted Beijing the detailed backgrounds and personal data of over twenty million federal employees, clearance-holders, and applicants, as well as that of their co-habitants and spouses, constituted one of the most damaging counterintelligence breaches in U.S. history. Assessing the loss, former Central Intelligence Agency (CIA) and National Security Agency (NSA) chief Michael Hayden offered a blunt, sobering take: "It remains a treasure trove of information that is available to the Chinese [Communist Party] until the people represented by that information age off. There's no fixing it." In his estimation, the impact of the breach would take a generation or more to fully subside, until the youngest members of the federal workforce at that time ultimately retired.[1]

Over the following decade, it would become clear that such counterintelligence hazards would hardly subside at all for reasons that were not yet fully evident, but still perhaps predictable. The aggregation of personal and location data on American consumers, including military service members, intelligence officers, national security officials, and contractors, would become part and parcel of the data-driven advertising behemoth that underpins the modern digital economy. While the threat of sophisticated cyber breaches into sensitive datasets remains, another trend is both an addition and contributor to the hacking risk: there is little need to steal

---

Justin Sherman *is the founder and CEO of Global Cyber Strategies, the scholar in residence at the Electronic Privacy Information Center, and a non¬resident senior fellow at the Atlantic Council.* ***Gavin Wilde*** *is a nonresident fellow at the Carnegie Endowment and Defense Priorities.*

through cunning espionage what can be obtained through little cost or effort in a vast and open data marketplace.

The question is whether such a status quo can be sustained without causing irrevocable damage to the counterintelligence interests of the United States. Can consumer data be treated as a "strategic resource," as the most recent National Counterintelligence Strategy asserts, from *both* the commercial and security perspectives simultaneously?[2] Or will one necessarily come at the expense of the other? As the age of "Big Data" and advances in computing have birthed the Artificial Intelligence era, these questions require urgent attention from policymakers. In what follows, we argue that they have, indeed, at critical points come into underappreciated but serious tension.

From OPM to Equifax to Salt Typhoon, the issue is now less that a single sensitive puzzle piece might be collected by U.S. adversaries but that a holistic mosaic has *already* been aggregated: that a vivid and detailed picture of U.S. military, intelligence, and national security rank-and-file personnel is coming into view for any sophisticated adversaries who care to look.

Military Jogging Routes and AdTech Targeting Packages

It's no secret that the entities that collect and store people's data are vulnerable to hacking. What is far less understood is the degree to which companies building and managing smartphones, laptops, mobile apps, websites, and myriad other digital technologies and interfaces all collect, aggregate, analyze, and share people's information. Jogging enthusiasts and open-source intelligence researchers brought this problem to the fore in 2018 when they revealed that Strava, a software application linked to FitBit devices, had been publicly posting the geolocations of its users. This oversight enabled curious online sleuths to watch U.S. military forces and intelligence officers in countries around the world as they jogged around forward operating bases and visited, presumably, safe houses.[3] While hardly a responsible privacy practice (even average runners might find their total run history, with timestamps, made available online without a password disturbing), what would have been an obvious, serious breach in a government context was the product instead of shockingly widespread industry data practices.

Corporations that are even less understood accelerate this personal data collection, aggregation, and analysis further. Companies that manage re-

al-time bidding networks—algorithmically run online auctions for other companies to buy "ad space" on an app, website, and so forth in order to show people ads—make reams of personal data available to countless entities sitting in the virtual auction house, on a constant basis, every single day.

Data brokers, those companies in the business of aggregating and selling people's data, likewise root their business, and as such their profit margins, on repeatedly selling information they've bought, compiled, and inferred to a wide range of buyers, largely at their own discretion.

Connected devices used by American consumers now routinely come with third-party software installed which transmits information about users, activity, and location to the digital advertising market—data brokers and bidding exchanges—to be packaged, traded, and sold. And companies that want to target people with particular messages, and then collect data on their responses, can leverage adtech companies to profile and reach individuals.

The prodigious volumes of data both collected *and* publicly available on data markets illustrate the remarkable extent to which Americans' personal information is rendered vulnerable to being hacked, stolen, and compromised. This fact alone should put OPM-style hacks into perspective. As NSA General Counsel April Doss wrote in 2020, governments pose but one facet of the challenge: "Data collected by national security programs [have come to] pale in comparison to the exquisitely detailed user profiles that are being amassed" either by, for, or on behalf of the U.S. tech sector.[4]

From Dating Apps to General Motors

A host of real-world events and civil society investigations from the post-OPM decade illustrate why the explosion of commercially available Big Data complicates and accelerates the counterintelligence dilemma facing the United States. Researchers have long demonstrated the ease of identifying, targeting, and even inducing U.S. and allied military service-members through their use of social media, dating, and messaging apps.[5] Their findings highlight the already high risks posed by poor organizational and operational security in the digital era.

More recently, a group of journalists outlined how even the most conscientious users, including those playing sensitive roles in government, intelligence, or the military, would be hard-pressed to extricate themselves from the digital ecosystem hard-wired into their devices. The team ac-

cessed geolocation and related data from in and around a U.S. military installation in Germany, one which is said to house, among other things, elements of America's nuclear arsenal and intelligence collection platforms. Their assessment is alarming: "Not only is [such] data collection likely capable of revealing military secrets, it is essentially unavoidable at the personal level. . . service members' lives being simply too intertwined with the technology permitting it."[6]

Attempts to cordon off specific locales from such data-harvesting are unlikely to alleviate such counterintelligence concerns. The vast majority of modern smart devices require some degree of geolocation data to function properly. Even if tech companies were prohibited from collecting and selling geolocation around specific sensitive facilities, the prohibition would fail to cover everywhere else affiliated personnel travel, everyone else they associate with, and everything else they do.[7] U.S. law generally requires an affirmative opt-in from users to collect and sell geolocation data, but this appears to serve more as a speed bump (or speeding ticket) rather than an adequate barrier against the targeting of U.S. officials and installations.[8] Just as the average citizen flies past the privacy policy and terms of service briefly popped onto their screens, clicking "agree" without so much as a substantive glance, so, too, do many U.S. government affiliates, rendering their supposed opt-ins just as illegitimate in practice. The Federal Trade Commission (FTC) has only historically taken a small number of enforcement actions against violators, most recently against General Motors.[9] Such actions, however, are mostly designed to bring offending organizations into full (or stricter) compliance with the law, while any punitive fines for unscrupulous activity ($51,744 per violation) are likely insufficient to serve as a deterrent in the broader multi-billion dollar digital advertising industry.[10]

The inability or unwillingness of the industry to police itself essentially means the data brokerage ecosystem can only be as ethically or legally respectful of consumer privacy as its least scrupulous participants. As legal scholar Andy Wang argues, "The magnitude of harm arising from one broker's activities depends on what data other brokers in the network are selling."[11]

Unlike tangible goods, data is an endlessly duplicable, non-exhaustible, and non-rivalrous good. A "tragedy of the commons" thus prevails: if one broker accumulates and sells nonconsensual or otherwise protected data, the compliance efforts of others can be mooted. Compounding the issue is that so-called know your customer (KYC) practices are either nonex-

istent or inconsistently applied throughout the data brokerage industry. According to a team of scholars from Duke University, "A malicious actor could easily lie their way around many data brokers' lax KYC controls, or simply find a broker with virtually no KYC practices whatsoever."[12]

Meanwhile, the promise that the data collected and aggregated on U.S. citizens can be safely and irreversibly "anonymized" has been repeatedly debunked as wishful thinking by researchers. For instance, a 2019 study at Imperial College, London, drew on just fifteen demographic attributes to reidentify U.S. citizens from an anonymized dataset, concluding that a composite picture of 99.98 percent of Americans could likewise be constituted, "seriously challeng[ing] the technical and legal adequacy of the de-identification release-and-forget model."[13] Nordic academics in 2021 likewise found that a year's worth of usage data by 3.5 million people from as few as four mobile apps was sufficient to reidentify 91.2 percent of them by cross-referencing publicly available information.[14] "Americans are the easiest to re-identify," the authors noted, raising the stakes in a society where only a small handful of companies control the entire mobile app ecosystem.

Endless hype cycles about AI and the future of the digital economy only further accelerate companies' efforts to collect vast amounts of information, aggregate and analyze disparate datasets, and monetize and sell data previously collected for a limited purpose. In other words, they accelerate the collection and dissemination of what is, at the end of the day, effectively exploitable intelligence on U.S. assets and personnel.

Protectionism, AI Competition, and Strategic Vulnerability

In 2025, national-level economic planning and industrial policy have largely shed the stigma that once surrounded them. As competition with China continues to intensify and a second Trump administration takes its stride, all eyes are on a U.S. tech sector that has achieved an almost mythical strategic significance. Beyond their innovative capacities, the U.S. federal bureaucracy and military-industrial complex have become widely dependent upon—if not inextricably linked with—the major tech multinationals, such as Microsoft, Google, Amazon, Palantir, Starlink, OpenAI, and others. The continued success of these firms is thus considered as much an issue of national security (however spurious those claims may be) as one of geoeconomic vitality.

But as the global scramble for data-fueled AI supremacy continues unabated, pitting the United States against its peer adversary, China, Washington has adopted a protectionist stance in just about every aspect but one: the ubiquitous collection and permissive availability of data on its citizens. Indeed, the United States is far and away the global leader in both the number of data categories available for purchase and the number of companies who provide them.[15]

Tech sector leaders are keenly aware of this fact. Like many other U.S. industries throughout history (particularly those wary of regulation that might curb anti-competitive or anti-consumer activity), the "national tech champion" card has long served as something of a free pass.[16]

Particularly in the era of hyper-competition for AI supremacy (however ill-defined the concept[18]), the U.S. tech sector has largely been victorious in its lobbying push to make the United States among the most permissive locales on earth to collect and trade data on consumers.[17] This is despite valiant cajoling by some privacy advocates, regulators, and legislators in recent years. This quintessentially American laissez-faire approach to online privacy has prompted individual states like California, Vermont, and others to take up the burden of introducing their own curbs on the unfettered agglomeration of personal data.[19] Valuable as they may be for individuals' privacy, such piecemeal endeavors are not enough in and of themselves to capture and curtail the wider canvas of personal data collection and sharing—and the counterintelligence risks that come with it.

Lacking much progress from Congress on a comprehensive privacy overhaul, successive administrations have attempted, however belatedly and piecemeal, to curb the outflow of sensitive data to adversaries through espionage or digital commerce. For instance, after the FitBit-related data leak of early 2018, the Department of Defense responded in August of that year by restricting the use of geolocation-enabled devices in areas of active military operations.[20] The directive ordered a broader risk assessment about digital geolocation, while Pentagon staff noted that enforcement of the order would be conducted on a "case-by-case basis."[21] By spring 2023, the Securities and Exchange Commission (SEC) had rolled out minimum cybersecurity standards and risk assessment guidelines for publicly traded companies.[22] The Biden White House had also issued an executive order forbidding the use of commercial spyware by U.S. departments and agencies in a bid to use federal purchasing power to constrain the burgeoning global market for sophisticated tracking and surveillance technologies.[23]

While these measures implicitly or indirectly nodded to the growing counterintelligence threat to U.S. officials and service-members, a subsequent Biden directive in 2024 was both more blunt and expansive. Executive Order (EO) 14117 tasked the attorney general with determining what kinds of data, irrespective of volume, could be exploited by specific adversarial states if linked to active or former federal employees, contractors, and sensitive government locations.[24] It additionally forbade the "bulk sale" of any nonpublic health, biometric, genomic, financial, and geolocation data that might be exploited by U.S. adversaries to identify and target individuals or groups (also delegating the task of defining "bulk" to the Department of Justice). Meanwhile, the Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB) made their initial forays into stricter enforcement of data broker activity later that year.[25]

However well-intended, these measures could prove fleeting from a political perspective, and easily circumventable from a practical one. The Trump administration moved quickly after it took office to weaken many of the agencies, like the CFPB, that it considers onerous for businesses or superfluous to the federal bureaucracy.[26] Data experts across academia, civil society, and industry-supporting law firms, meanwhile, widely predict that many of the most significant cybersecurity, spyware, and data-protection initiatives from previous years are likely to be deliberately scrapped by the Trump White House, if not simply left to atrophy.[27] But from a purely counterintelligence perspective, experts are also quick to point out that previous measures merely acted like Band-Aids on a gaping wound.

This is because the structural focus of EO 14117 and its congressional cousin, the Protecting Americans' Data from Foreign Adversaries Act of 2024 (or PADFAA, for short), on "cross-border data-flows" is too narrowly scoped, with the key terms being too arbitrarily defined to serve as a meaningful safeguard. Both documents focus squarely on preventing specific adversarial countries, such as China and Iran, as well as any firms controlled in some part by their citizens, from obtaining sensitive troves of data about U.S. entities.

But in both instances, the stress on volume, direct transfers, and specific categories of data overlook the many pathways that can otherwise be taken to accumulate the data needed to build a comprehensive mosaic. Peter Swire and Samm Sacks, writing for *Lawfare*, draw parallels with money laundering: "Years of effort have gone into detection and regulation of 'structuring' transactions, to prevent the small from adding up to

the big. [But it] will be a long and uncertain path to build similar rules for data sales."[28] These measures fail to consider the spider webs of indirect purchases, diversions, and well-obscured fronts—common in the intelligence business for circumventing sanctions and export controls—that foreign adversaries could wield to buy up reams of data indirectly from U.S. firms.[29] These fail to tackle the deeper causes of this stubborn phenomenon of data porousness, such as highly unregulated data broker sales and poorly regulated online advertising practices, making government actors ill-equipped to handle the full spectrum of privacy issues, let alone complex national security risk.

And, perhaps most crucially, these concomitant programs struggle to grapple with the intersections between privacy and national security. The executive branch has, for instance, relegated the task of inspecting consumer data transfers with a national security risk to the Justice Department's National Security Division, meaning that inspectors operate without comprehensive federal privacy and security laws to stand on. Another policy decision has effectively given some national security data authority to the FTC, an agency well-versed in complex data technologies and predatory adtech practices, but one lacking the resources, expertise, and integration with intelligence and law enforcement agencies necessary to tackle nation-state exploitation of data.

Confronting the Dilemma

If policymakers' speeches and industry lobbying points are to be believed, commercial data is a strategic resource necessary to "win" the "AI race" with China. This argument demands continued widespread, unfettered, permissionless corporate access to vast troves of data (so the rhetoric goes). Not only consumer data should be accessible, but data held (and, in many cases, copyrighted by) corporations, research institutions, and other entities, too—all of which can be funneled into corporate AI systems, turbocharged into the military and national security apparatus, and used to gain a competitive edge, particularly against Beijing.

Indeed, there are plentiful ways that commercial data and open-source intelligence can be used to advance national security objectives and fulfill what many would agree are important governmental functions, such as hunting foreign hackers or investigating Russian war crimes in Ukraine.[30] Yet, the conundrum lies in the copious national security and counterintelligence problems embedded throughout the practically unrestrained

private-sector data collection landscape. However much might be gained by this (often nakedly self-serving) appeal to the national interest as the trump card against stronger AI and data regulations, there are too few incentives to consider what has already been lost: any semblance of anonymity, obscurity, or privacy that once enabled sensitive government entities to function safely.

Ultimately, policymakers must come to terms with the fact that U.S. national security officials, military service members, intelligence officers, and sensitive facilities worldwide already operate at a major disadvantage in the face of both state and nonstate adversaries alike. This vulnerability will only grow with time as long as we have few meaningful protections against data-brokers and other types of unfettered data collection, transmission, and use. Protecting service members from espionage, blackmail, sabotage, or worse will mean confronting a stark reality: piecemeal policing at the post-collection stage like that attempted by previous administrations cannot achieve what even a modest federal data privacy framework could. Taming the adtech market will require a great deal of political will, particularly in response to objections from would-be "national champions."[31] But the decade since the OPM hack has made one thing clear: data-dependent tech companies can champion the national economy or they can champion the national security bureaucracy, but doing the former through race-to-the-bottom data hoarding and sale will only put the latter in even greater jeopardy. AA

Notes

1. Dan Verton, "Impact of OPM Breach Could Last More than 40 Years," *FedScoop*, July 10, 2015.
2. Liz Sly, "U.S. Soldiers Are Revealing Sensitive and Dangerous Information by Jogging," *Washington Post*, January 29, 2018.
3. Tim Hwang, *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet* (New York: Farrar, Straus and Giroux, 2020); Jesse Frederik and Maurits Martijn, "The New Dot Com Bubble Is Here: It's Called Online Advertising," *Correspondent*, November 6, 2019.
4. April Falcon Doss, *Cyber Privacy: Who Has Your Data and Why You Should Care* (Dallas: BenBella Books, 2020).
5. Issie Lapowsky, "NATO Group Catfished Soldiers to Prove a Point About Privacy," *Wired*, February 18; Frank X. Hartle et al., "The Impact of Social Media Geolocation on National Security and Law Enforcement," *Issues in Information Systems* 23, no. 1 (2022): 204–13.
6. Dhruv Mehrotra and Dell Cameron, "Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany," *Wired*, November 19, 2024.
7. Justin Sherman, "Data Brokers and Threats to Government Employees," *Lawfare*, October 22, 2024.

[8] For a primer, see: Stacey Gray and Pollyanna Sanderson, "Policy Brief: Location Data Under Existing Privacy Laws," Future of Privacy Forum, December 2020.

[9] Federal Trade Commission, "FTC Takes Action against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data without Consent," news release, January 16, 2025.

[10] Federal Trade Commission, "FTC Takes Action against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites," news release, December 2, 2024.

[11] Andy Z. Wang, "Network Harms," *University of Chicago Law Review* 91, no. 7 (November 2024): 2093–137.

[12] Brady Kruse, "How Congress Can Rein in Data Brokers," *CyberScoop*, December 20, 2023.

[13] Luc Rocher, Julien M. Hendrickx, and Yves-Alexandre de Montjoye, "Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models," *Nature Communications* 10, no. 1 (July 23, 2019): 3069.

[14] Vedran Sekara, Laura Alessandretti, Enys Mones, and Håkan Jonsson, "Temporal and Cultural Limits of Privacy in Smartphone App Usage," *Scientific Reports* 11, no. 1 (2021).

[15] Henrik Twetman and Gundars Bergmans-Korats, *Data Brokers and Security: Risks and Vulnerabilities Related to Commercially Available Data* (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2020).

[16] Robert Kuttner, "Global Capitalists or National Champions?," *American Prospect*, October 17, 2023.

[17] Heather Roff, "The Frame Problem: The AI 'Arms Race' Isn't One," *Bulletin of the Atomic Scientists* 75, no. 3 (April 2019): 1–4.

[18] Dell Cameron, "Surprise! The Latest 'Comprehensive' US Privacy Bill Is Doomed," *Wired*, June 27, 2024.

[19] Jeremy Crampton, "The U.S. Government Must Protect Citizens from Geolocational Disinformation and Surveillance AI," Scholars Strategy Network, January 31, 2024.

[20] Craig Timberg, "Lawmakers Demand Answers about Strava 'Heat Map' Revealing Military Sites," *Washington Post*, January 31, 2018.

[21] Lauren Williams, "DOD Sharply Restricts Use of Geolocation Devices and Services," *Defense One*, August 8, 2018

[22] SEC staff, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," U.S. Securities and Exchange Commission, July 26, 2023.

[23] Mark Mazzetti, "Biden Acts to Restrict U.S. Government Use of Spyware," *New York Times*, March 27, 2023.

[24] Mark Febrizio, "Biden's Ambitious Executive Order Does More for Data Security than Banning TikTok," George Washington University Regulatory Studies Center, April 26, 2024.

[25] Electronic Privacy Information Center, "FTC Takes Action Against Data Brokers for Selling Sensitive Location Data," December 3, 2024.

[26] Lesley Stahl, "Trump, DOGE Work to Shutter CFPB, an Agency Created in Response to the 2008 Financial Crisis," CBS News, February 23, 2025.

[27] Eric Geller, "More Spyware, Fewer Rules: What Trump's Return Means for US Cybersecurity," *Wired*, November 14, 2024.

[28] Peter Swire and Samm Sacks, "Limiting Data Broker Sales in the Name of U.S. National Security: Questions on Substance and Messaging," *Lawfare*, February 29, 2024.
[29] Justin Sherman, "Data Brokerage and the Third-Country National Security Problem," *Lawfare*, April 16, 2025.
[30] Lindsay Freeman, "Digital Evidence and War Crimes Prosecutions: The Impact of Digital Technologies on International Criminal Investigations and Trials," *Fordham International Law Journal* 41, no. 2 (2018).
[31] Henry Farrell and Abraham Newman, "What Happens When Tech Bros Run National Security," *TIME*, September 20, 2023.

This article originally appeared in American Affairs *Volume IX, Number 2 (Summer 2025): 156–65.*

Exploitable by Design: Social Media and the AdTech Threat

by Emerson T. Brooking

One way to conduct an online influence operation is to recruit a team of professional propagandists and engineers, build a vast network of fake social media accounts, plant a series of false or inflammatory narratives, and continuously collect intelligence to adjust the operation in real time. Another way is to buy some online ads and let large social media platforms do each of these things for you.

Most Americans are not primed to think of advertising as a national security concern. Instead, online advertising is a business and a very large one at that. Nearly $330 billion dollars will be funneled into online ads in 2026. By 2031, the market will climb to more than $500 billion.[1] More than a third of this spending is concentrated in North America.[2] American firms dominate this market, and American eyes are by far its most lucrative target. A single Facebook ad delivered to an American consumer is worth roughly twice as much as the same ad delivered to someone in the United Kingdom or Germany; nearly seven times that of someone in India.[3]

With so much money at stake, it is little wonder that the technology and infrastructure responsible for delivering these ads ("adtech") is stuck in a perpetual arms race for human attention. The world of social media advertising, with which this article is principally concerned, is dominated by Meta, Google, to a lesser extent, X, and the awkwardly bifurcated ByteDance and "TikTok USDS Joint Venture LLC. Each of these entities must constantly engineer new ways to keep users glued to their services, incentivize at least a subset of users to constantly generate new content,

Emerson T. Brooking *is a resident senior fellow at the Digital Forensic Research Lab (DFRLab) of the Atlantic Council Technology Programs.*

and entice advertisers by exposing their users' data in the most maximally intrusive and minimally compliant way possible.

Ironically, this is where the word "advertising" sells the whole thing short. Yes, one can use the most powerful behavioral targeting apparatus ever built to move endless dropshipped t-shirts or particle board furniture. But from the perspective of hostile foreign states, who have spent more than a decade engaged in information warfare campaigns against U.S. citizens and interests, social media adtech is not a way to make money.[4] Instead, it is an obvious and exceptionally attractive weapon.

The United States has never permitted foreign governments such unfettered access to American information infrastructure. Yet today, and in sharp contrast with the active U.S. regulation of radio and television, social media companies have no legal obligation to disclose who is purchasing ads aimed at American citizens, nor to flag foreign-funded ad buys in real time. Indeed, their only real obligation is to periodically show up to be yelled at by the Congress and to promise, next time, to do better.

This regulatory weakness has nothing to do with the "unique" properties of the internet and social media, which are now older and better established than either the radio or television at the time that they were given their own basic regulatory regimes. Instead, it is a matter of money and power. Large social media companies have spent more than $250 million dollars since 2020 alone to sustain this total regulatory vacuum.[5] In some cases, social media companies have worked to perpetuate this U.S. vulnerability even as they waged a years-long campaign to portray TikTok as a dire national security threat.[6]

What follows is an exploration of the machinery of social media advertising, the century-old norms it has been permitted to evade, and the hostile foreign intelligence operations that have sought to turn this machinery toward their own ends. There are clear precedents and ready proposals to close it. What is missing, as it has been for nearly thirty years, is political will.

An Invisible and Insatiable Machine

One surreal aspect of social media advertising is that, although at least half the world's population is intimately familiar with it, its business model remains essentially invisible. Most social media users will see social media ads as an annoyance layered onto a communications platform, the same way that commercials interrupt a TV show. In reality, the advertisements

are the product. The communications platform—whether an X doomscroll, an inscrutable Facebook newsfeed, or a short-form video treadmill of TikTok or YouTube Shorts—is just an inducement for users to hand over the data that makes the advertising work.[7]

This machine is insatiable by design. Somewhere around the early 2010s, social media companies collectively realized that the user data they were gathering to improve their products could also be bundled and sold to third parties. This is what media scholar Shoshana Zuboff describes as "behavioral surplus": the vast residue of user activity that can be safely packaged for sale.[8] Once companies came to rely on this data harvesting for revenue, metrics like user satisfaction, security, or even growth became secondary concerns.

The targeting that this data enables can be breathtakingly precise. Although Facebook is not the only platform of concern, it is the platform about which the most is known, and therefore the easiest point of reference. Advertisers using the Meta Ads Manager can upload a spreadsheet of email addresses or phone numbers to build a "Custom Audience" matched against the platform's roughly three billion users.[9] It takes only a few more clicks to generate a "Lookalike Audience" of hundreds or millions, inferred from shared page likes, ad interactions, social proximity, and numerous other tiny indicators that remain one of Meta's most closely guarded secrets.

These audience groupings are automatic and occasionally quite embarrassing. In 2017, ProPublica found that Facebook had packaged "Jew haters" as a targetable advertising category, because enough users had listed it as an interest.[10] Although social media platforms have since taken steps to prohibit obviously harmful or illegal audience segmentation (one cannot explicitly advertise to "Jew haters" today, just as one cannot advertise housing to only persons of color), the vastness of available data invites new kinds of malicious use. By combining thousands of different "proxy attributes," it remains possible and profitable to target Americans on the basis of race, sexual orientation, or religion.[11]

These finely sliced ads are essentially invisible to anyone outside of their target audience. The industry term is "dark posts": ads that appear only in the feeds of selected users, leave no trace on the advertiser's public pages, and vanish once the campaign ends.[12] On Facebook and Instagram, they are called "Unpublished Page Post Ads."[13] X, TikTok, and YouTube offer equivalent capabilities through their respective ad managers. In practice,

an advertiser can serve dozens (or hundreds) of different ads to different audience segments without publicly appearing to run any ads at all.

Social media platforms do not like opening these systems to public scrutiny. After the 2016 U.S. election, Meta and Twitter both launched ad transparency archives. The subsequent decade has seen their hollowing out or abandonment. After Elon Musk acquired Twitter in 2023, the newly renamed X quickly gave up on its transparency tools, especially advertising disclosures. Meanwhile, Meta's ads library seems obsolete by design. The tool reveals only when an advertisement is running. It is not possible to view old data or past campaigns, to see how an audience was selected, or to understand how different ads running at the same time may be targeting different groups of people.

Although Meta discloses more information about ads regarding "social issues, elections, or politics," this is still a voluntary commitment bounded by inconsistently applied definitions.[14] A 2019 investigation by my own Digital Forensic Research Lab found that Facebook allowed multiple ad buys from Chinese state television, intended to demoralize Americans about a potential trade war while never classifying them as "political" at all.[15] Even when debated in good faith, the question of what constitutes a "social" ad can also be tremendously tricky. An ad promoting reproductive health is liable to meet the "social" threshold; an ad selling prescription birth control is not.[16]

Nonetheless, Meta may still be the most transparent of the bunch. Google waited until 2018 to launch its own advertising archive, which remains altogether less reliable and useful, revealing obvious sponsored content but not what videos are targeting certain user demographics. TikTok conspicuously avoided launching a real U.S.-focused ads transparency center, even when U.S. criticism of the platform had reached fever pitch.[17]

In all cases, this sluggishness is deliberate. The elements that make social media advertising so immensely lucrative—the precise audience identification and segmentation, the invisibility and untraceability—are directly at odds with any level of public disclosure. In this industry, transparency is always bad for business.

Used as Intended

Lack of transparency is hardly an impediment to the foreign intelligence operatives and state media apparatchiks who today seek to manipulate U.S. public opinion online. Since roughly 2012, when Iranian propagan-

dists first used pseudonymous pages to push cartoons boosting Ron Paul's longshot Republican bid, these information operations have grown dramatically in both volume and sophistication.[18] So has foreign propagandists' interest in using social media advertising to automate parts of their job.

The most infamous example of this occurred between 2015 and 2017, when Russian contractors spent around $100,000 to purchase roughly three thousand microtargeted Facebook ads, intended to draw Americans into a mishmash of fake pages that alternately promoted black liberation, secessionism, or the campaign of then candidate Donald Trump.[19] Maryland received the most such ads, focusing on Baltimore and surrounding areas. One campaign cost 3,700 rubles (roughly $58) to promote a "Demand Justice for Freddie Gray" event at the Baltimore City Circuit Courthouse, purchased less than two months after Gray's death.[20] Those few confused citizens who did turn out soon dissipated after discovering neither basic structure nor leadership at the gathering. The Russians who orchestrated this operation, an operation that ultimately reached 11.4 million Americans in paid ads, did so as Facebook customers, not hackers. They simply used Facebook, in the words of Evgeny Morozov, "as it was always intended to be used."[21]

Although Iran and China have used their own clandestine advertising to target Americans, they have also sought to harness the U.S. social media ecosystem to do the work for them.[22] When Facebook purged one such Iranian network in 2018, it removed more than eighty pages, groups, and accounts that had posed as American liberals, much of their content aimed squarely at the sitting president. Iran has used ad tools to steer audiences in more than two dozen countries toward its state media apparatus, dodging U.S. sanctions in the process.[23]

During the 2019 Hong Kong protests, Chinese state outlets *Xinhua* and *China Daily* paid Twitter to promote dozens of tweets portraying the pro-democracy demonstrators as "violent" thugs showing "signs of terrorism."[24] This content included a crude cartoon of a protestor holding a Molotov cocktail in one hand and an American flag in the other. Facebook identified similar campaigns from Chinese state media targeting audiences across Hong Kong and Southeast Asia.[25] The campaign was brazen enough for Twitter and Facebook to announce sharp limits on state media advertising.[26] For many more years, however, Chinese state media remained free to build and propagandize to an audience via organic discovery.

While foreign propagandists' exploitation of social media adtech is both normatively troubling and academically interesting, it is reasonable to ask how much this all matters. After all, the sum of clandestine ad spending by Russia, China, and Iran over the past decade almost certainly does not exceed $1 million dollars—roughly what the Coca-Cola Corporation spends on digital advertising every three hours.[27] Moreover, social media's role in political opinion formation remains largely unsettled. It is certainly not the case, as was sometimes insinuated in the aftermath of the 2016 election, that each American exposed to Russian propaganda had their beliefs shifted in some meaningful way. The overwhelming majority neither noticed nor cared.

But just as with social media users' tendency to think of ads as an annoying interruption (instead of the product itself), it is altogether too kind to these companies to measure their platforms' exploitation by foreign actors through direct ad purchases alone. The $100,000 that Russia spent on Facebook advertising between 2015 and 2017, for instance, was just one small piece of a customer acquisition strategy that involved tens of thousands of fake social media assets and which, at the end of its 194-week run, had reached the Facebook feeds of 126 million Americans.[28] Along the way, Facebook was not just collecting rubles to serve Russian propaganda to U.S. citizens. It was also charging American companies to advertise alongside this Russian-fabricated content and tracking Americans' engagement with the material to commodify and sell their data later.

Indeed, social media platforms' business model means that they materially benefit from all sorts of foreign state exploitation, just as they provide these propaganda efforts with essential enabling infrastructure. This is the common thread that binds together episodes like "Spamouflage," a massive influence network of at least 8,500 Facebook assets, linked to Chinese law enforcement and identified in 2024; a sprawling thirteen thousand-account anti-Ukraine TikTok network orchestrated by Russia and discovered in late 2023; and an Iran-directed Instagram spam campaign that flooded the Trump family with death threats after the January 2020 assassination of Iranian general Qassem Soleimani.[29]

In some cases, the sheer amount of cash that one can earn from commodifying American attention has led purely profit-motivated actors to adopt the same tools and tactics of these political propagandists. This is why, during the 2016 U.S. election, so many young men in North Macedonia took to operating mostly pro-Trump content mills, and why

so many highly partisan and apparently American accounts on X are operated from Africa and Southeast Asia today.[30]

In each of these real or quasi-propaganda campaigns, social media companies sit at the center, profiting from every side of the transaction. They sell ads to help grow fake pages and accounts, sell more ads against the engagement that these assets generate, and monetize all the valuable "behavioral surplus" that these operations leave behind. These companies may be sincere in wanting to block this activity from their services, but unsurprisingly, they are also united in the belief that they and only they can address the problems unleashed by their own business models.

Recent Ancient History

This is a remarkable conceit and a largely ahistorical one. For most of the twentieth century, the United States treated the question of foreign access to American communications infrastructure as essentially settled. The answer, supplied by the active oversight of the U.S. government, was "no." This answer stood even as the United States pioneered a standard of media freedom and individual speech rights that would become the envy of the world.

Indeed, when Secretary of Commerce Herbert Hoover convened the first National Radio Conference in 1922, his concern was not foreign propaganda but the medium's commercial capture. "It is inconceivable that we should allow so great a possibility for service to be drowned in advertising chatter," he told the assembled broadcasters.[31] By 1925, Hoover was less concerned by the dominion of the advertisers than by the collusion of the "speechmakers" to the exclusion of everyone else from the air.[32] Congress acted on this logic with the Radio Act of 1927, which created the Federal Radio Commission and established that broadcasters must operate in "the public interest, convenience, and necessity." The Act included a blanket ban on foreign ownership of broadcast licenses, a provision that attracted no recorded opposition and has never been repealed.[33]

This prohibition was further codified by Section 310 of the Communications Act of 1934. No alien, no foreign corporation, and no entity with more than 20 percent foreign ownership could hold a broadcast license. The newly established Federal Communications Commission (FCC) was explicit about its task to "thwart the airing of foreign propaganda" by broadcast licensees who otherwise "exercise[d] editorial discretion over the content of their transmissions."[34] The Foreign Agents

Registration Act (FARA) of 1938 extended a parallel logic to political advocacy on American soil, compelling foreign agents to disclose their activities and label their propaganda materials so that Americans would always know when they were being addressed by a foreign power.[35]

These basic radio and television regulations remain in place today. As recently as January 2026, the FCC unanimously voted to strengthen this framework, requiring every broadcast licensee in the United States to follow stringent new disclosure requirements for firms owned just 10 percent by entities in China, Russia, Iran, North Korea, Cuba, or Venezuela.[36]

Meanwhile, the most powerful broadcasting tools in world history remain wholly exempted from this or any other sort of meaningful regulation. Social media companies do not owe this privileged position to principled arguments or technical necessity. Instead, they have simply excelled at preventing regulation from being discussed at all.

Anything is Too Much

How did the internet get off so easy? The short answer is familiar to readers of this journal: a bipartisan consensus, forged in the Clinton administration and defended by Bush, Obama, and Trump in turn, held that the internet was fundamentally different than prior communications technologies and that its extraordinary potential might be smothered by any amount of state intervention. Section 230 of the Communications Decency Act immunized platforms from liability for user-generated content, while concurrent legal decisions found that private platforms were exercising First Amendment editorial discretion in whatever manner they chose to restrict the speech of their users. The Telecommunications Act of 1996 deregulated the broader industry, while the Federal Trade Commission would spend many years studiously avoiding any meaningful exercise of jurisdiction over digital advertising.[37]

Yet even the most committed internet exceptionalist might have expected the United States to require foreign governments to disclose their purchase of political advertisements on U.S. social media, and for these American companies to limit their instrumentalization by hostile state propagandists. But that did not happen either.

This, in essence, was all the Honest Ads Act proposed. Introduced in 2017 by Senators Amy Klobuchar, Mark Warner, and John McCain, the bill would have compelled digital platforms to follow the same disclosure requirements that have governed radio and television advertising

since 1971.[38] Online platforms with more than 50 million monthly visitors would maintain a public file of political ad purchases exceeding $500, including the identity of the purchaser. Foreign nationals would be explicitly prohibited from buying political ads, as they have long been prohibited from buying broadcast time. The bill was endorsed, at least in public, by Meta, Twitter, and Google.

Yet even this mildest of corrective measures has never become law or even survived a vote on the House floor. The Honest Ads Act was introduced in every Congress between 2017 and 2024, either as standalone legislation or as a component of broader reform packages.[39] It quietly died each time.

The most straightforward explanation for this failure is money. In 2024 alone, Meta spent $24.4 million on federal lobbying and employed eighty-five registered lobbyists, roughly one for every six members of Congress.[40] Through this intensive lobbying effort, social media platforms essentially strangled the Honest Ads Act while never wavering in their public support. Testifying before Congress in April 2018, Mark Zuckerberg publicly endorsed the bill, calling foreign interference, "a problem that's bigger than anyone one platform."[41] Simultaneously, Meta lobbyists were working the phones to make sure it never got a vote.[42] Meanwhile, the voluntary ads transparency measures announced by Meta, Twitter, and Google (and discussed earlier in this essay) enabled sympathetic lawmakers to declare that legislation was unnecessary in the face of effective self-regulation.

But self-regulation lasts only as long as the pressure does. Following Trump's 2024 re-election, in which the threat of formal regulation was replaced with an ever-shifting mix of coercion and cajolement, the mask came off quickly. In the United States, it is considerably harder to identify foreign state propaganda activity on social media than it was a decade ago, with researchers stymied by poor data and increasingly obsolete transparency tools. Beyond U.S. borders, the situation is even more fraught. In July 2025, Meta decided to withdraw entirely from the European political ads market rather than comply with the European Union's new political advertising disclosure requirements.[43] Google went further, quietly deleting a database that researchers and journalists had relied upon to track foreign spending in twenty-seven EU countries.[44]

Yet the U.S. Congress works in mysterious ways. Although it failed to seed any effective regulations for the global communications revolution, nor to account for even very basic remedies to limit the threat of foreign interference, it did manage, very confusedly, to ban TikTok.

Double Standards or None

In January 2025, the Supreme Court unanimously upheld a law compelling TikTok to divest from its Chinese parent company, ByteDance, or face a ban in the United States.[45] The Court found the government's interest in preventing "a foreign adversary from collecting vast swaths of sensitive data about the 170 million U.S. persons who use TikTok" as sufficiently compelling to survive First Amendment challenge. Yet the resulting deal, finalized in January 2026 at approximately $14 billion dollars, revealed how narrowly the threat had been defined. Even as American investors assumed ownership of the U.S. TikTok (TikTok USDS Joint Venture LLC), ByteDance would still control "e-commerce, advertising, and marketing" on the new platform.[46] In other words, the systems that enable and incentivize foreign interference in the first place were essentially carved out.

Just as the TikTok deal was closing, Reuters obtained internal Meta documents revealing that the company had earned $18 billion dollars in advertising revenue from Chinese clients in 2024: 11 percent of its global income, more than doubling in just two years.[47] Nearly a fifth of this revenue came from advertisements for scams, illegal gambling, and other content that violated Meta's own policies. When an internal anti-fraud team threatened to create too much friction for Chinese advertisers, Mark Zuckerberg ordered it disbanded.

The bipartisan argument for banning TikTok, an argument driven partly by Meta lobbyists, was that a Chinese-owned platform capable of microtargeting Americans posed an unacceptable national security risk. But even as Congress worked to neutralize the theoretical threat of a Chinese-owned platform, Meta was collecting billions from Chinese clients who were already known to be exploiting their advertising infrastructure, all while avoiding scrutinizing their activities too closely, much less disclosing them in a proactive and transparent way.

This is the glaring contradiction at the heart of American internet policy. Congress determined, on a bipartisan basis, that a foreign-owned platform's capacity to collect data on and aggregate content for American citizens constituted an intolerable threat to national security. Yet throughout this period, the U.S.-owned infrastructure through which Russia, China, and Iran had sought to manipulate American citizens for over a decade went essentially unconsidered. The Honest Ads Act, which would have extended the mildest version of a century-old broadcast disclosures to social media, never survived a vote in the House, while the TikTok ban

sailed through both chambers. TikTok—routing the data of 170 million Americans through a digital ecosystem ultimately answerable to Beijing—certainly did demand scrutiny. But if TikTok represented a severe national security threat, other U.S. companies do too.

We do not need novel remedies to address foreign state exploitation of social media. All we need, really, is a bit of consistency. The same disclosure requirements that have governed broadcast advertising since 1971 should be applied, with a few changes, to digital platforms. The ad transparency archives that Meta and Google built largely for show should be replaced by a public repository that no company can delete in a fit of pique. And more of us—especially those of us with very different political orientations and visions for the future of the country—should agree that these companies have given far too little while taking altogether too much from American public life.

These are either American companies with clear obligations to the American people, or they are stateless profit machines that deserve no special protections from American policymakers. They should not be permitted to have it both ways. AA

Notes

1 "Online Advertising Market Size, Share Analysis & Industry Research Report, 2031," Mordor Intelligence, accessed June 2026.

2 Mordor Intelligence, "Online Advertising Market," accessed June 2026.

3 "Facebook CPM by Country," Lebesgue, accessed June 2026.

4 P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York: Houghton Mifflin Harcourt, 2018).

5 Alix Fraser et al., "The Tech Money Machine: How Silicon Valley Buys Power — and Shapes Reality," *Tech Policy Press, May 22, 2025.*

6 Taylor Lorenz, Drew Harwell, "Facebook Paid GOP Firm to Malign TikTok," *Washington Post,* March 30, 2022.

7 Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: PublicAffairs, 2019).

8 Zuboff, *The Age of Surveillance Capitalism, 75.*

9 Naveen Kumar, "Facebook Users Statistics 2026 - Global Data & Growth Trends," *DemandSage,* May 7, 2026.

10 Julia Angwin, Madeleine Varner, and Ariana Tobin, "Facebook Enabled Advertisers to Reach 'Jew Haters,'" *ProPublica*, September 14, 2017.

11 Piotr Sapiezynski et al., "On the Use of Proxies in Political Ad Targeting," arXiv, October 18, 2024.

12 Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford: Oxford University Press, 2018).

13 "Creating Facebook Unpublished/Dark Posts," *Brandwatch Help Center, February 2, 2026.*

14 "Ads about Social Issues, Elections or Politics," Meta, accessed June 2026.

[15] Donara Barojan, "Made in China: Economic Influence Operations," *DFRLab, February 7, 2019.*
[16] Lisa Femia, "Decoding Meta's Advertising Policies for Abortion Content," Electronic Frontier Foundation, September 30, 2025.
[17] Brandon Silverman, "How Transparent Is TikTok?" *Some Good Trouble*, March 16, 2023.
[18] Ben Nimmo, et al., "Iran's Broadcaster: Inauthentic Behavior," *Graphika*, May 5, 2020.
[19] Alex Stamos, "An Update on Information Operations on Facebook," *Facebook Newsroom*, September 6, 2017.
[20] John Fritze, "House Committee Releases Russian-Linked Ad Depicting Freddie Gray," *Baltimore Sun*, November 1, 2017.
[21] Evgeny Morozov, "Capitalism's New Clothes," *Baffler*, no. 43 (January 2019).
[22] FireEye Intelligence, "Suspected Iranian Influence Operation Leverages Network of Inauthentic News Sites & Social Media Targeting Audiences in U.S., UK, Latin America, Middle East," *FireEye*, August 21, 2018; Billy Perrigo, "Exclusive: How a Chinese Influence Operation Spent $30,000 on U.S. Facebook and Instagram Ads," *Time*, March 28, 2023.
[23] Estimated from eight Meta attributions of Iranian campaigns, August 2018–March 2025. See Emerson Brooking and Suzanne Kianpour, *Iran's Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century* (Washington D.C.: Atlantic Council, 2020).
[24] Ryan Mac and Rosalind Adams, "Have You Seen These Ads About Hong Kong's Protests? China Certainly Hopes You Have," *BuzzFeed News*, August 19, 2019.
[25] Mac and Adams, "Have You Seen These Ads About Hong Kong's Protests? China Certainly Hopes You Have."
[26] Twitter Safety, "Information Operations Directed at Hong Kong," Twitter Blog, August 19, 2019; Kate Conger, Raymond Zhong, "Facebook and Twitter Say China Is Spreading Disinformation in Hong Kong," *New York Times,* August 20, 2019.
[27] "Coca-Cola Co.—Ad Spending, Facts and Profile," *Ad Age*, updated December 10, 2025.
[28] Renée DiResta et al., "The Tactics & Tropes of the Internet Research Agency," New Knowledge, prepared for the Senate Select Committee on Intelligence, December 17, 2018.
[29] "Quarterly Adversarial Threat Report, Third Quarter 2023," Meta, November 2023; Roman Osadchuk, "Massive Russian Influence Operation Targeted Former Ukrainian Defense Minister on TikTok," *DFRLab*, December 14, 2023*; DFRLab,* "Tensions Escalate on Social Media Platforms after Soleimani's Death," *DFRLab*, January 4, 2020.
[30] Heather C. Hughes, Israel Waismel-Manor, "The Macedonian Fake News Industry and the 2016 US Election," *PS: Political Science & Politics 54, no. 1 (January 2021);* "Partisan US-Seeming Accounts Run from Africa and Southeast Asia," BBC News, [date unverified], accessed June 2026.
[31] Herbert Hoover, "Address to the First National Radio Conference," U.S. Department of Commerce, February 27, 1922.
[32] Herbert Hoover, "Address to the Fourth National Radio Conference," U.S. Department of Commerce, November 9, 1925.

[33] Mark Goodman, "The Radio Act of 1927 as a Product of Progressivism," *Media History Monographs* 2, no. 2 (1999); Radio Act of 1927, Pub. L. No. 69-632, 44 Stat. 1162 (Feb. 23, 1927).

[34] FCC staff, "Review of the Commission's Regulations Governing Television Broadcasting; Market Entry and Ownership Rules," Federal Communications Commission, NPRM, 10 FCC Rcd 4873 (1995), para. 99; "Review of Foreign Ownership Policies for Broadcast, Common Carrier and Aeronautical Radio Licensees under Section 310(b)(4) of the Communications Act of 1934, as Amended," Federal Communications Commission, Report and Order, FCC 13-150 (2013).

[35] Philip M. Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, 3rd ed. (Manchester: Manchester University Press, 2003).

[36] "Foreign Adversary Attestation and Disclosure Requirements," Report and Order, FCC 26-3, Federal Communications Commission, January 29, 2026.

[37] Tim Wu, The Master Switch: *The Rise and Fall of Information Empires* (New York: Alfred A. Knopf, 2010); Siva Vaidhyanathan, *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy* (Oxford: Oxford University Press, 2018); Josh Hawley, *The Tyranny of Big Tech* (Washington, D.C.: Regnery Publishing, 2021).

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

[39] Mark R. Warner, Amy Klobuchar, and Lindsey Graham, "Warner, Klobuchar, Graham Reintroduce Honest Ads Act," press release, U.S. Senate, February 27, 2023. The bill had been introduced in every Congress since the 115th (2017), originally co-sponsored by John McCain; Graham assumed McCain's role following McCain's death in 2018. Provisions were also incorporated into the For the People Act and Freedom to Vote Act. The bill was not reintroduced in the 119th Congress.

[40] "Meta Platforms: Lobbying Profile, 2024," OpenSecrets, accessed February 2026.

[41] Mark Zuckerberg, testimony before the U.S. House Committee on Energy and Commerce, *Facebook: Transparency and Use of Consumer Data*, 115th Cong., 2nd sess., April 11, 2018.

[42] Heather Timmons and Hanna Kozlowska, "Facebook's Quiet Battle to Kill the First Transparency Law for Online Political Ads," *Quartz*, March 22, 2018.

[43] "Ending Political, Electoral and Social Issue Advertising in the EU," Meta, July 25, 2025.

[44] Samantha Cole, "Google Just Removed Seven Years of Political Advertising History," *404 Media*, November 26, 2024.

[45] *TikTok Inc. v. Garland*, 604 U.S. ___ (2025) (per curiam), upholding Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), Pub. L. 118-50, div. H (2024); Gorsuch, J., concurring in the judgment. U.S. Supreme Court, January 17, 2025.

[46] David Shepardson, "TikTok Seals Deal for New US Joint Venture to Avoid American Ban," Reuters, January 23, 2026.

[47] Jeff Horwitz, Engen Tham, "Meta tolerates rampant ad fraud from China to safeguard billions in revenue," Reuters, December 15, 2025.

The Factory Floor Is Now the Battlefield

by Joshua Steinman

Last September, a Chinese state-sponsored hacking group used an AI model to run a cyber espionage campaign against roughly thirty targets across the globe, including chemical manufacturers. The operation took place at machine speed and confirmed what many researchers had been saying for years: that large language models would reshape the cybersecurity landscape.

Less than one year later, Anthropic released Mythos, a frontier AI model able to autonomously discover exploits in nearly any system or network. OpenAI's latest model has similar capabilities, and the open-source models are only a few months behind. What previously took a nation-state to do will soon be achievable with a few hundred dollars of tokens.

For the past twenty years, attacking industrial systems required years of specialized training, custom tooling, and a nation-state budget. That model is now dead. Today, it takes a laptop and an internet connection. Welcome to "the Infinite Front." American firms should take note.

The Chinese have been preparing for this day for a long time. Volt Typhoon, a Beijing-linked group, has maintained persistent access to a broad swath of American critical infrastructure for years. The Department of Homeland Security openly talks about how this group is likely pre-positioning to disrupt industrial systems in the event of a conflict over Taiwan.[1]

At an electric and water utility in Littleton, Massachusetts, Volt Typhoon sat inside the operational technology network for roughly three hundred days while they exfiltrated geographic information system (GIS)

Joshua Steinman *is cofounder of Galvanick, an industrial cybersecurity company. He is a former Navy officer turned investor and served on the National Security Council staff from 2017–2021.*

data and spatial layouts necessary to conduct targeted cyber attacks; the utility only found out about the breach when the FBI called to notify them.[2]

Volt Typhoon and similar Chinese-backed hacking groups are already using AI tools to radically accelerate the breadth and speed with which they operate. And the security through obscurity that industrial systems and networks have enjoyed for the past forty years is coming to an end.

In response to this new threat environment, there are three priorities American industrial firms must adopt now, not next quarter. The first is to maximize compliance. Frameworks such as Cybersecurity Maturity Model Certification (CMMC), if taken seriously and not as a box-checking exercise, can serve as a roadmap to a minimally viable security program.

The second is to instrument the factory floor. Firewalls are important, but most activity happens on endpoints. While monitoring industrial networks is important, it is just as important to watch the actual computers performing critical tasks, from engineering workstations to industrial controllers. Most attacker activity happens on these endpoints, and monitoring them can be done passively without touching production.

The third is to remember that security is, at the end of the day, a human task. Basic security training works. Whether it is anti-phishing training or the regular reminder to make sure every person in the office has a correct and working badge, firms need to train their people to be the first line of defense. AA

Notes

1 "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure [Alert Code: AA24-038A]," Cybersecurity and Infrastructure Security Agency, February 7, 2024.

2 For more details on this incident, see: Jonathan Grieg, "Volt Typhoon Hackers were in Massachusetts Utility's Systems for 10 Months," *Record,* March 12, 2025.

How to Safeguard America's Critical Infrastructure

by Lars Erik Schönander, Joshua Levine, and Adam Gluck

The world is increasingly awash with cybersecurity incidents. In 2025, Americans alone lost over $20 billion in cybercrimes.[1] Globally, cybersecurity incidents are becoming more common by the year, and attacks targeting civilian infrastructure have become a regular facet of warfare. Since the Maidan Revolution of 2014, Ukraine has been targeted by Russian hackers attempting to cripple their infrastructure, while Iranian hackers have infiltrated critical infrastructure across the United States amid the recent war.[2]

Often, the specific target of these hacks is a niche part in a factory that, for example, controls circuit breakers. But why are these niche parts targeted, and what makes them uniquely vulnerable to cyberattacks? In short, the world's physical infrastructure is built on technology that—while excellent for industrial automation, the tasks it solves—was not built for a world in which every device is connected to the internet.

Operational Technology (OT) is hardware and software that interacts with physical systems. A classic example of OT hardware is a programmable logic controller (PLC), a type of computer designed to automate industrial processes. PLCs were invented in the 1960s to replace more cumbersome forms of industrial automation that many automotive companies possessed at the time.[3] They are a key component of any modern factory and make mass production possible.

A whole layer of digital OT facilitates the security and functionality of the physical OT. Network segmentation software ensures that machines are only accessed by authorized users and protocols. Asset management

---

Lars Erik Schönander *is a business operations lead at Copia Automation.* ***Joshua Levine*** *is director of technology and statecraft at the Foundation for American Innovation.* ***Adam Gluck*** *is the CEO of Copia Automation.*

software helps firms audit and track all the OT that they control. Finally, if a hack happens, backup and disaster recovery software enables companies and governments to get their systems back up and running rapidly.

Infrastructure that the world depends on runs through these machines and the digital safety net behind them. Food processors use PLCs to automate ingredient mixing. Water treatment plants use sensors to monitor water tanks and ensure the right chemical mix enters the water to make it clean. Power plants use control systems to regulate how generators and turbines run to produce electricity. It's easy to imagine how the failure of these systems can produce horrific results. Food processors become unable to make food. Water treatment plants suddenly produce toxic water. Power plants break down, and thousands to millions are affected. Our critical infrastructure could be crippled in countless other ways, owing to the diversity of industries that use OT.

If the consequences of the failure of these machines are so dire, why are they vulnerable? Unfortunately, in industry and government, funds are not available to help construct the digital architecture required to protect our physical infrastructure, which was constructed in a bygone threat landscape. Threat actors are becoming ever more sophisticated in how they hack these systems. Simultaneously, the threat of frontier AI models such as Mythos looms over the horizon, foreshadowing a future in which threat actors have access to frontier models that can easily overwhelm companies and countries without equivalent access. We must rapidly and resolutely prepare for these urgent threats against our critical infrastructure.

No Money for Security

Even the United States, home to some of the world's most successful cybersecurity companies, struggles with implementing cybersecurity infrastructure. Firms and government agencies, particularly at the state and local level, unfortunately do not spend money to secure their IT/OT infrastructure because of disincentives and/or a lack of funds for infrastructure upgrades.

Firms are disincentivized to spend on cybersecurity broadly because it's an operating expense, not a capital expense. While more flexible than capex spending, cyber opex strikes executives as a cost-center, which does not motivate them to spend on it. As for OT security spending, the status quo is even worse because OT budgets are split between multiple professionals with different spending priorities.[4]

Equally, one of the most common challenges that state-level chief information security officers (CISOs) face is lack of budget.[5] A plurality of CISOs reported that their budgets for cybersecurity either stayed the same as last year or was reduced.[6] Funding is even worse at the local level. For example, the Center for Internet Security (CIS), in its 2024 report, found that of the thousands of local agencies that reported their cyber capabilities, 32 percent were not performing any cybersecurity activities at all or doing them on an ad hoc basis.[7]

Unsurprisingly, underfunding allows for hacks that cripple organizations. In 2024, Russian hackers breached the water system for a small town in Texas, causing water tanks to flood for nearly an hour.[8] Understandably, the local government did not have the budget to protect against this. The city did not even learn about the hack from a city employee but from a software vendor notification. The town's entire revenue in 2023 was $3.37 million, with no dedicated line item for cybersecurity.[9] Overflowing water tanks may seem like a minor threat, but they hint at the access rival powers have to our basic utilities and the catastrophic damage they can inflict. As we have seen in Ukraine, the cost of major OT hacks can be deadly.

Operational Technology as a Target in Warfare

Discussions of large-scale hacks into civilian infrastructure are not idle speculation; they are a major facet of contemporary warfare. Ukraine is the poster child victim of these attacks as the country has dealt with hacks to civilian OT infrastructure for over ten years. After the failure of Russian interests in the Maidan Revolution and the cessation of the Donbas war, Russia continually attacked Ukrainian infrastructure. One of the most infamous state-sponsored hacker groups, Sandworm, has been at the forefront of these attacks on Ukrainian critical infrastructure.[10] In 2015, the group used the BlackEnergy malware to hack into SCADA systems in western Ukraine. With access to the substations, they were able to open the station circuit breakers and break the power grid for hundreds of thousands of Ukrainians. Such attacks were repeated at the start of the Russia-Ukraine war. In April 2022, with the Industroyer2 virus, Sandworm crippled the Ukrainian power grid by shutting off multiple electrical substations, leading to the loss of power for over two million Ukrainians.[11]

Beyond being a terror tactic, Russia hacking Ukrainian power grids is a way to cripple the Ukrainian war effort. There are specific reasons why the

Ukrainian power grid is so vulnerable. Poor cybersecurity is the simplest example. Russian hackers were able to shut down power for Ukrainians in the dead of winter with the FrostyGoop malware because the power system was connected to a router directly connected to the internet. With no internal IT security, the hackers could easily wreak havoc by accessing the connected systems.[12]

Worse, many pieces of OT infrastructure were never even built with security in mind. These systems were not intended for a world of seamless interconnectivity. Modbus, an industrial communication protocol from the 1970s, is a good example: it was built for reliability in isolated factory environments, not for a world in which critical infrastructure is connected to the internet and laid bare by state-backed hackers. When Sandworm deployed FrostyGoop malware against a Ukrainian district's heating provider, they exploited exactly that flaw. They sent Modbus commands to shut down the power generation systems, cutting off heat for civilians in the dead of winter.[13]

Outdated OT can also make infrastructure more vulnerable. In 2015, for example, Ukrainian power companies experienced major outages after Russian hackers corrupted the firmware on serial-to-Ethernet converters at electrical substations. These cables exist to enable communication between old and new devices.[14] Unfortunately, the serial equipment is often insecure, and the actual converters tend to have a variety of vulnerabilities. In the case of the 2015 hack, the vulnerability is one that the Department of Homeland Security flagged back in 2008. It's easy to know that an issue exists, but remediating a legacy OT environment issue can take years, if the will is even mustered to undertake such a project at all.

A different kind of vulnerability occurs when outdated OT is forced to work in ways for which it was never intended. With the 2024 FrostyGoop hack, once the Russians infiltrated the Ukrainian IT system, they successfully manipulated the OT. Once they hacked into the PLCs, they prevented users from monitoring how those PLCs were operating.[15]

After years of attacks, Ukraine today represents an optimistic case. Through experience, Ukrainians have been well-trained and are now highly motivated to fix all cybersecurity issues within their infrastructure. The threat is existential. Much less can be said of companies and countries elsewhere who remain lax in their security; their folly could be catastrophic.

The United States is now getting a taste of these Russia-style OT attacks due to the war with Iran. Already, American OT has been directly

targeted by Iranian-backed hacker groups.[16] Specifically, they are targeting Rockwell Automation/Allen-Bradley PLCs, which has directly led to PLC disruptions across multiple sites.

This is not the first time Iranian hackers have decided to hack into American critical infrastructure. Back in 2023, a water treatment plant in Pennsylvania was hacked by CyberAv3ngers, an Iranian-backed hacker group.[17]

At the start of the U.S.-Iran war, the Iranians hacked the medical company Stryker. The hack deleted hundreds of thousands of accounts and disrupted internal communication systems.[18] The cause of the hack? A single compromised admin account for Microsoft Intune which allowed hackers to shut down all devices managed on that system.[19] If a Fortune 500 company has these vulnerabilities, imagine the ineptitude of most American firms, possessing even less money, resources, and training, in dealing with sophisticated hacks from state-backed actors. Now imagine every anti-American actor having access to tools that enable them to commit crippling attacks at scale.

The Frontier Model Threat

Back in April, Anthropic launched Mythos, a specialized model for cybersecurity work. What they publicly reported has dark implications for everyone's security. Anthropic's Red Team, in their preview of the model, found that it successfully located and exploited zero-day vulnerabilities in every major operating system and was capable of writing sophisticated exploits.[20] OpenAI has also launched a similar model.[21] While the two leading frontier labs are trying to ensure these models do not break the internet through Glasswing and Daybreak respectively, OT systems will still face a variety of challenges because of these models.

To start, security by obscurity is officially over. AI models can rapidly find and exploit bugs in the wild.[22] While the diversity of OT equipment used to be something that deterred hackers, this is no longer a barrier. A Mythos-tier model can easily discover and exploit vulnerabilities in these oft-neglected systems.[23] And it is unlikely that, say, a municipal water plant will have access to the technology and training needed to patch these issues.

Barring safeguards, models with these types of capabilities will be accessible to everyone. Open-source AI models such as DeepSeek and Kimi are roughly four months behind the state-of-the-art models.[24] Unlike

American AI companies, Chinese AI model companies such as DeepSeek, Kimi, MiniMax, and Z have not launched equivalent cyber programs.

Already, however, we can see that open-source models are nearly as effective at cyber compared to their closed-source counterparts. An independent safety evaluation of Kimi2.5 revealed that the model had cyber capabilities on par with closed-source models.[25] A similar evaluation found the same with DeepSeek v4.[26] That level of performance is only a baseline; presumably, the open-source models will keep improving. Now imagine an improved version of one of these models, with its guardrails removed, deployed against American industry and business. If Stryker can be crippled with a single hacked admin account, what disasters could a hacker create with a model that lets one rapidly develop and deploy new exploits?

Cyber Solutions

Thankfully, there are steps the government can take today to defend against these risks and ensure the security of American industry. To start, the Trump administration can ensure its own OT systems are ready for adversarial advanced AI. The administration recently released an executive order on artificial intelligence, one section of which focused on improving the cyber defense of our national security systems.[27] The administration must ensure that OT security in these systems, such as industrial control systems on military bases for water and power, is upgraded.

Equally lucky for CISOs and firms looking to secure their operations, there is an existing policy lever that is useful: the tax code. Rather than trying to set formal requirements for cybersecurity spending or formalize existing guidance, a better path forward is to lean into existing financial incentives to make investing in IT/OT easier. This approach is a win-win: firms will be empowered to invest in improving their operations and embrace a flexible, iterative approach to governing connected systems without creating additional regulatory burdens across the economy.

To enable this step-change in preparedness, industry and government should look to existing incentives. The distinction between capex and opex is relevant because cybersecurity has traditionally been viewed as the latter, which dissuades firms from investing in this area. Taking a creative approach to the tax code offers an opportunity to solve this problem with private dollars rather than creating a cumbersome government grant program or expanding regulatory authority.

The biggest opportunity for this "creative reading" was created by updates in President Trump's One Big Beautiful Bill Act (OBBBA). Starting with hardware and physical systems, the law enables 100 percent bonus depreciation for eligible MACRS property with a recovery period of twenty years or less. This covers a broad swath of components, systems, sensors, and other kinds of equipment. Another opportunity is the 100 percent allowance for qualified production property, which is narrower, but still useful for physical system investments and upgrading. Finally, there is Section 179, which provides elective immediate expensing for tangible property, such as machinery and equipment. The full deduction is capped at $2.5 million per purchase, with reduced dollar-for-dollar expensing up to $4 million, before phasing out after $6.5 million. To secure critical infrastructure and take advantage of software-enabled systems, which have been billed as key for reindustrialization and advanced manufacturing, firms must invest and iteratively improve their plant. OBBBAlays the foundation to do so.

Moving to firmware and software development, there are three notable sections of the IRC that come into play. First is Section 174A, which allows for full expensing and deduction for software development spending. Firms looking to develop new connected systems with cyber-relevant software and firmware should be eligible for full expensing. Development is key, which creates a mutually beneficial opportunity of exchange: firms providing IT/OT services have a ready market and chance to develop solutions tailored to customer needs while the purchaser is incentivized to invest in needed capacity consistently over time.

Together, these several lines of the tax code can be the key to unlocking necessary investment in IT/OT capabilities. Ensuring that these investments can be made now and sustained over the long term is critical for securing American industrial operations moving forward. Guidance from the White House, in the form of an executive order, in tandem with guidance from Treasury and the Office of Management and Budget, can set a standard for the duration of this administration, and hopefully, into the future. Providing this clarity is necessary as cyber threats evolve, IT/OT systems become increasingly vulnerable, and the opportunity cost of inaction thereby grows. Done right, these investments can simultaneously stimulate and secure the techno-industrial platforms of the future. AA

NOTES

1 2025 Internet Crime Report, Federal Bureau of Investigation, 2025.

2 Significant Cyber Incidents," Center for Strategic and International Studies, March, 2026; "Iranian-Affiliated Cyber Actors Exploit Programmable Logic

Controllers Across US Critical Infrastructure," Cybersecurity & Infrastructure Security Agency, April 7, 2026.

3 Ken Ball, "How Programmable Logic Controllers Emerged from Industry Needs," Control Engineering, September 1, 2008.

4 Dean Parsons,"2025 ICS/OT Cybersecurity Budget: Spending Trends, Challenges, and the Future," SANS Institute, March 2025.

5 Meredith Ward, Mike Wyatt, "2026 NASCIO-Deloitte Cybersecurity Study," Deloitte Center for Government Insights, April 27, 2026.

6 Ward and Wyatt, "2026 NASCIO-Deloitte Cybersecurity Study."

7 Ward and Wyatt, "2026 NASCIO-Deloitte Cybersecurity Study."

8 Ken Miller, "Rural Texas Towns Report Cyberattacks That Caused One Water System to Overflow," Texas Tribune, April 19, 2024.

9 Colt Ellis et al., "2022–2023 Approved Budget," City of Muleshoe, October 1, 2022.

10 "Sandworm Team, Group G0034," MITRE ATT&CK, December 4, 2024.

11 Andy Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine," *Wired*, April 12, 2022.

12 Eduard Kovacs, "FrostyGoop ICS Malware Left Ukrainian City's Residents Without Heating," *SecurityWeek*, July 23, 2024.

13 Greenberg, "Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine."

14 "Cyber-Attack Against Ukrainian Critical Infrastructure," Cybersecurity & Infrastructure Security Agency, February 25, 2016.

15 Pierluigi Paganini, "FrostyGoop ICS Malware Targets Ukraine," Security Affairs, July 23, 2024.

16 "Cyber-Attack Against Ukrainian Critical Infrastructure," Cybersecurity & Infrastructure Security Agency.

17 Erika Stanish, "Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group," CBS News, November 26, 2023.

18 Lynsey Chutel, "Cyberattack Adds to Fears of New Front in Iran War," *New York Times*, March 12, 2026.

19 Andrej Safundzic, "The Stryker Hack: How One Compromised Admin Account Led to 200,000 Wiped Devices," *Lumos*, March 15, 2026.

20 Nicholas Carlini et al., "Assessing Claude Mythos Preview's Cybersecurity Capabilities," Anthropic, April 7, 2026.

21 "Introducing Trusted Access for Cyber," OpenAI, February 5, 2026.

22 Larry O'Brien, "Should Industrial Cyber Teams Be Concerned About Claude Mythos and Project Glasswing?" ARC Advisory Group, April 20 2026.

23 Jordyn Alger, "What Are Security Experts Saying About Claude Mythos and Project Glasswing?" *Security Magazine*, April 10, 2026.

24 Jack Edwards, Luke Emberson, "Open Models Lag State-of-the-Art Closed Models by 4 Months," Epoch AI, May 29, 2026.

25 Zhen-Xin Yong et al., "An Independent Safety Evaluation of Kimi K2.5," arXiv, April 3, 2026.

26 "Evaluating DeepSeek v4 Pro for Frontier Risks," Neo Research, May 29, 2026.

27 Donald J. Trump, "Promoting Advanced Artificial Intelligence Innovation and Security," White House, June 2, 2026.

"I've Been Scammed, Now What?": The Growing Crisis Facing Everyday Americans

by Haiman Wong

On a normal summer day in June, Manny Guerrero, a soft-spoken Vietnam War veteran living in Las Vegas, picked up the phone and was told he had beaten the odds and won. The voice on the other end claimed to be from Publishers Clearing House and quickly painted a vivid picture: a check for $3,500,000, a new 2024 BMW XM SUV, balloons, and even a big party delivered to his front door if he'd like. All he had to do was cover the taxes up front.[1]

None of this sounded entirely unreasonable or implausible. After all, when Manny was looking for something to take his mind off the death of his wife in 2008, he started ordering items from Publishers Clearing House, hoping he could win money by being entered in their sweepstakes. So, Manny leaned in. He started writing checks and wiring money: $22,000, $30,000, $40,000 at a time. Before he knew it, $180,000 was gone.

Manny hadn't told anyone about his win, not even his daughters. He planned to surprise them. Manny intended to use his winnings to fix up his house and leave behind an inheritance for his children. Instead, his daughters received a different kind of surprise when an FBI agent called to inform them that their father had been the victim of a scam.

Shortly after, Manny's daughter, Debbie, asked his credit union why no red flags were raised when her father started making large withdrawals repeatedly—and why she and her sister, who were both listed on the account, were not at least notified. In response, the credit union simply told her that the money was her father's, and he was free to do what he wanted.

***Haiman Wong** is a resident fellow at the R Street Institute's Cybersecurity and Emerging Threats team.*

With no way to recoup the lost money, Manny ultimately resorted to taking out a $25,000 loan to stay afloat.

Manny's story would be tragic even if it were rare. But unfortunately, it's not. According to the Pew Research Center, 75 percent of American adults, across age groups, have experienced some kind of online scam or attack.[2]

To make matters worse, scammers are increasingly targeting American veterans. As of June 2025, nearly nine in ten servicemembers and veterans have been targeted by a military service-related scam over the past twelve months, according to data from the American Association of Retired Persons (AARP).[3] American seniors are also a favorite target for scammers, with the FBI's Internet Crime Complaint Center receiving 147,127 fraud complaints from individuals over sixty in 2024, which constitutes a 46 percent increase from 2023.[4] While these numbers may seem overwhelming in and of themselves, they only reflect the losses that we know about: a growing number of victims opt to forgo reporting their experiences altogether due to shame, a fear of blame or disbelief, and the high difficulty of successfully prosecuting scams that often cross legal jurisdictions.[5]

All of this reinforces how what happened to Manny wasn't just the result of misfortune, one bad actor, or a single moment of poor judgment. It was the product of a well-oiled machine, one that successfully blends breached data, social engineering, and minimal institutional friction to extract money at scale. For every Manny, there are thousands more, each targeted through tailored scripts designed to exploit people when they are vulnerable.

Treating stories like Manny's as though they are isolated incidents misses the broader reality. Fraud and scams are a growing national crisis: one that has been shaped by our data practices; evolved alongside our emerging technologies; and reinforced by the limits of our current oversight, enforcement, and response systems.

To understand the scale of what we are all up against, and to determine what meaningful action looks like, we need to look more closely at how we got here and what today's threat landscape really looks like.

The Origins and Features of Today's Threat Landscape

The terms *fraud* and *scam* are frequently used interchangeably. While both terms are often used correctly to describe a scenario where a victim loses

money under false pretenses, each term actually refers to a different strategy used by bad actors.

Financial fraud generally refers to dishonest or deceptive methods used to acquire information or cause financial harm, such as identity theft, SIM swapping, or payment card fraud.[6] In contrast, scams are usually schemes designed to trick individuals into willingly providing money or sensitive information.[7] Many attackers use social engineering in their scams, which is the tactic of manipulating, influencing, or deceiving a victim to gain control over a computer system, or to steal personal and financial information.[8] For example, in romance scams, a bad actor will create fake profiles on dating websites or apps, form a relationship with a target to build trust by communicating regularly, and then eventually start asking for money.[9] Bad actors may say they need the money to travel to meet their target in person for the first time or because an emergency has occurred. They may also initiate contact outside of dating platforms through popular social media platforms like Instagram or Facebook. Regardless of what a romance scam looks like, the outcome is generally the same: a broken heart, lost time, and stolen money. Other types of scams that have grown in popularity are employment scams, charity scams, and the sale of nonexistent goods or services scams, among others.[10]

The scam is a recurring phenomenon throughout American history. In the 1840s, a sharply dressed New Yorker named William Thompson roamed the streets striking up friendly conversations with strangers he passed by.[11] After establishing rapport, Thompson would ask whether they had "confidence" in him, just enough to entrust him with their watch or other valuables until the next day. While most declined, some agreed and Thompson would never return their valuables.[12] Thompson's tactics earned him the moniker "the Confidence Man," a term popularized by reporter James Houston in the *New-York Herald* in 1849, and the origin of what we now more readily recognize today as the "con man."[13] Though Thompson was eventually arrested and mocked by his contemporaries for the clumsiness of his tactics, the case did reveal an enduring truth: successful scams exploit trust and often rely on creating a sense of urgency or pressure, so that the target feels cornered into making a decision swiftly.

Throughout history, fraud and scams were relatively hit or miss, constrained by friction. Physical proximity, slower communication, and limited reach imposed natural barriers on scale and repetition. Schemes required face-to-face interaction, handwritten correspondence, or extended coordination—conditions that carried high time costs and

personal risk. Fraud and scams existed, but it was episodic rather than industrial.

Those constraints eroded as society digitized. As banking, commerce, and government services moved online, so did fraud and scams, not because deception itself evolved, but because the environment did. Each wave of digital transformation expanded access to money and information while reducing the effort required to exploit both. The gradual shift from mail-based communication to electronic transactions and online accounts enabled fraud and scams to occur around the clock, across institutions, and eventually, even across the borders of nation-states.[14] At the same time, the growth of large-scale data creation and collection—through public records, commercial intermediaries, and data breaches—made it easier for bad actors to identify, profile, and target potential victims with specificity.[15]

In other words, the difference in today's threat landscape lies in the information (data) and tools (technologies) now available to those conducting these schemes. What once required postage stamps or live callers can now be scaled to millions with a single script or email blast.[16]

Today, financial fraud and scams operate largely in digital spaces through robocalls, phishing emails, smishing texts, spoofed websites, and social media outreach.[17] With vast amounts of personal information accessible online, bad actors can also target victims with unprecedented precision.[18] Automation and artificial intelligence (AI) have lowered the cost of execution, enabling schemes to spread faster and appear more convincing.[19] In some regions, scam operations have even become a full-fledged industry. Organized crime groups in Myanmar, Cambodia, and Laos have taken advantage of ongoing political instability to run large-scale cyber scam businesses.[20] These scam centers are often staffed with trafficked labor and used to target victims around the world with fraudulent investment pitches and impersonation schemes. According to the FBI, Americans lost an estimated $2.6 billion to scams like these in 2022 alone.[21]

Governments around the world have already begun to treat cyber scam operations not only as criminal enterprises, but as national security threats. In recent years, China and Thailand have led repatriation efforts targeting the traffickers and operators behind scam centers.[22] Meanwhile, the United States, Canada, and the United Kingdom have issued coordinated sanctions and ramped up cryptocurrency investigations and asset seizures in an effort to disrupt financial flows.[23] While these actions have yielded some high-profile successes, experts caution that such victories re-

main uneven and often short-lived. As long as the incentives remain high and enforcement remains fragmented, scam operations are likely to stay highly mobile, technologically adaptive, and capable of scattering across legal jurisdictions to evade accountability, evolving faster and with greater ease than the systems trying to stop them.

How Scammers and Fraudsters Think, Target, and Profit

Not every fraudster or scammer is committing cybercrime by choice. As illustrated in the previous section, some of the people sending phishing texts are victims themselves, trafficked into scam compounds and forced to work under constant threat of violence. Their "motive," if it can even be called that, is survival.

But for others, cybercrime is not only a choice, it is a profession. Some scammers operate independently, while others function as affiliates or contractors within larger syndicates. These criminal networks often resemble legitimate businesses, complete with specialized roles, performance targets, structured workdays, and even paid time off.[24] Some cybercriminals focus on direct engagement with targets through impersonation or romance scams. Others build and sell tools or offer services like malware kits, fake landing pages, stolen credentials, distributed denial of service or DDoS-for-hire, and money laundering, to lower the barrier of entry for less sophisticated threat actors.[25] In each case, the goal is the same: scale the operation, maximize success, and minimize risk.

Success, in turn, depends on access to data. Personal information scraped from public records, harvested in data breaches, or purchased on the dark web helps scammers profile potential victims and tailor their approach.[26] A leaked email might be used for phishing. A public Facebook or LinkedIn post could offer valuable insight into an individual's goals, interests, or life events that make someone more emotionally sensitive to psychological urgency. Something as simple as a birthday could help attackers bypass initial security questions aimed to verify an individual's identity when they expand the scope of their targeting to other accounts owned by the individual. All of this helps attackers improve the precision of their targeting and increase the success rate of their operations.

Sometimes, this targeting isn't just precise, it's refined over time.[27] In multiple federal cases in the United States, data brokers were caught knowingly selling lists to scammers and incorporating scammer feedback into their models.[28] One firm, Epsilon Data Management, provided data

on more than 30 million Americans to scammers over nearly a decade.[29] Others, like Macromark and KBM Group, reportedly went as far as partnering with scammers to improve profiling algorithms—turning revictimization into a lucrative business model.[30]

Once a victim engages, monetization can happen in a few different ways.[31] Some targets are coaxed into sending wire transfers, gift cards, or cryptocurrency. Others have their credentials harvested, their bank or benefits accounts drained, or their identities stolen. Stolen data is often repackaged and resold, fueling the next wave of scams.[32] Once laundered, the profits can be reinvested into upgrading existing infrastructure or hiring more personnel.

Nation-state threat actors have also turned to financially motivated cybercrime. In some cases, these campaigns are explicitly designed to generate revenue. For example, North Korean operatives routinely compromise crypto wallets and exchanges to funnel revenue toward the regime's weapons development and sanction evasion efforts.[33] In other cases, cybercrime enables broader state objectives. Chinese espionage groups have reportedly supplemented their campaigns by monetizing stolen data, while Russia has turned to criminal actors to support its war in Ukraine.[34] As the lines continue to blur, cybercrime is increasingly both a revenue stream and an operational enabler for advanced persistent state-backed threats, supplementing broader campaigns of espionage, disruption, and influence.

Where Law Enforcement Falls Short

When someone realizes they have been defrauded or scammed, the guidance they receive is often centralized and procedural, particularly in the first twenty-four to seventy-two hours. Victims are encouraged to stop communicating with the fraudster or scammer, immediately notify their bank, account manager, or payment provider, secure compromised and vulnerable accounts, reset passwords, and document what happened to the best of their ability.[35] Many are also advised to file reports with the Federal Trade Commission or the FBI's Internet Crime Complaint Center, and in some cases, to contact local law enforcement or a state attorney general's office to formally report the incident.[36]

These recommended best practices are well intentioned and can sometimes materially influence how widespread the damage becomes. Acting quickly can help prevent additional breaches and monetary losses, preserve evidence, and alert financial institutions to suspicious activity. This guid-

ance also reflects how fraud and scams are handled today across banks, technology companies, and law enforcement agencies at the local, state, and federal levels. For victims navigating shock, confusion, and urgency, these steps offer a sense of direction in a moment when the rug has been pulled out from underneath them, often without warning or ceremony.

At the same time, this default guidance often reveals the limits of the system victims are being asked to rely on. The sobering reality is that once funds are transferred, especially through wire services, gift cards, cryptocurrency, or accounts routed overseas, recovery is rare.[37] Local police departments, while often the first point of contact, typically lack the jurisdiction or technical capacity to pursue cases that cross state or national boundaries.[38] State legislative offices may receive complaints or requests for assistance from constituents, yet face similar constraints when suspected perpetrators and payment pathways extend far beyond their scope of authority.[39] Even at the federal level, agencies contend with overwhelming caseloads, fragmented data, and limited resources to trace funds that move rapidly between bad actors and across platforms or borders.[40]

The challenge is further compounded by attribution: perpetrators frequently obfuscate their identities, operate across jurisdictions, and rapidly change tactics, meaning investigative leads can go cold as techniques evolve in days or weeks rather than months or years.[41] In practice, many reports function primarily to document harm and raise awareness rather than to reverse losses or deliver substantive resolution.[42]

Over time, this dynamic can discourage reporting altogether, reinforcing undercounting and weakening the data that institutions, policymakers, and law enforcement rely on to understand emerging threats.[43] As these experiences compound, trust in digital communications, financial systems, and public institutions begins to erode, making everyday interactions and decisions more fraught and defensive.[44]

None of this reflects a lack of concern or effort from law enforcement, public officials, or industry. Rather, it underscores a fundamental mismatch between the scale and speed of modern scams and the systems available to address them. Fraud and scams today are digital, distributed, and transnational. Enforcement, by contrast, remains largely reactive, jurisdiction-bound, and resource-constrained. Attribution is difficult, recovery is unlikely, and accountability often lags behind innovation.

The result is a response framework that is forced to prioritize damage control over meaningful remediation. For victims, that gap can feel like resignation. For institutions, it exposes structural limitations. Taken to-

gether, these constraints help explain why so many Americans feel that even when they do everything they are told to do, the outcome still falls short.

Where Policy Can Move the Needle

Encouragingly, combatting financial fraud and scams has emerged as a rare area of bipartisan focus, driven by the growing recognition that these crimes do not discriminate by income, geography, or political affiliation—and that, left unaddressed, they not only harm individual Americans but also threaten our national security.

At the federal level, recent legislative proposals reflect a clearer understanding of both the scale of the crisis and the structural weaknesses in the current responses and resources available to Americans. Senators Mike Crapo (R-Idaho) and Mark Warner (D-Virginia), joined by Jerry Moran (R-Kansas) and Raphael Warnock (D-Georgia), introduced the Task Force for Recognizing and Averting Payment Scams (TRAPS) Act in June 2025 to create a standing interagency body spanning the Treasury Department, Consumer Financial Protection Bureau, Federal Communications Commission, Federal Trade Commission, Department of Justice, prudential regulators, and industry representatives.[45] Rather than imposing new compliance requirements, the task force model focuses on coordination: clarifying institutional roles, improving information sharing, and identifying gaps that might prevent agencies from acting effectively in concert.[46] In doing so, the TRAPS Act has the potential to provide federal leadership and strategic direction across agencies that too often operate in silos rather than as a team toward a shared mission.

Complementing this approach, the Guarding Unprotected Aging Retirees from Deception (GUARD) Act, emphasizes capacity-building over rulemaking.[47] Introduced on a bipartisan basis by Representatives Zach Nunn (R-Iowa), Scott Fitzgerald (R-Wisconsin), and Josh Gottheimer (D-New Jersey) in April 2025, the proposed bill would expand permissible uses of existing Department of Justice grant funding, allowing state, local, tribal, and federal law enforcement agencies to invest in hiring more investigative staff, modern forensic tooling such as blockchain analytics, and cross-jurisdictional coordination.[48] By focusing on practical enablement rather than rigid new mandates, the GUARD Act reflects a pragmatic understanding of where policy can most realistically improve outcomes in an environment defined by speed, scale, and cross-border complexity.

Still, until legislative measures such as the TRAPS Act and the GUARD Act are enacted—and in the absence of a coherent national strategy—industry has largely been left to shoulder the operational burden of response. Financial institutions, in particular, have strong incentives to protect their consumers from falling victim to frauds and scams and have invested heavily in education campaigns, enhanced authentication, behavioral monitoring, transaction delay mechanisms, and dedicated fraud response teams responsible for identifying and interrupting suspicious activity earlier in the transaction lifecycle.[49] These efforts reflect years of learning under constant pressure from evolving scam tactics and shifting consumer behavior.

Some policy debates, however, risk misdiagnosing where responsibility and leverage most effectively reside.[50] Financial institutions are often treated as the natural locus of liability because they handle the movement of funds. In reality though, banks are more often the final destination in a much longer chain of deception that originates elsewhere—on social media platforms, over telecommunications networks, through spoofed identities, and via sustained psychological manipulation or emotional appeal that occurs entirely outside the financial system.[51]

Policy approaches that default to liability shifting or mandatory reimbursement for consumer-authorized transactions may be well intentioned, but they focus narrowly on the endpoint of a scam, leaving the upstream ecosystem largely intact. Over time, that can narrow the menu of viable defenses by pushing institutions toward compliance-driven controls rather than toward proactive prevention, early intervention investments, and ongoing adaptive solutions that actually reduce harm.[52] When incentives tilt in this direction, collaboration, initiative, and defense ultimately suffer, even as fraud and scam vectors themselves continue to evolve.

The Role of Emerging Technologies

Beyond clearer guidance, better coordination, and capacity-building, effective policy must also recognize and support the role that emerging technologies increasingly play in combatting fraudsters and scammers. Although it can be tempting to view technology as the primary driver of fraud and scams, its responsible deployment remains one of the most effective tools for early detection, real-time response, and post-incident recovery.[53]

At the consumer level, artificial intelligence is already shifting fraud prevention from reactive clean-up to more timely intervention. Instead of relying primarily on spam filters or consumer reports, newer fraud prevention systems learn what "normal" looks like for an individual user and assess the severity of a potential risk when behavior meaningfully deviates from that baseline.[54] Sudden changes in login activity, unusual payment requests, atypical transaction routing, or patterns inconsistent with prior behavior can trigger temporary account freezes.[55] Moreover, on-device protections recently launched by major technology companies are designed to detect suspicious phone and text conversations in real time, alerting users when requests or questions resemble known scam tactics and advising them to pause or exit the conversation.[56] While these brief interruptions may only last a few seconds, they can be enough to disrupt the urgency scammers rely on and give consumers the space to reconsider before funds or sensitive information are exchanged.[57]

At the enforcement and recovery level, AI-enabled forensic tools now allow investigators to sift through and correlate large volumes of transaction data, communications metadata, platform activity, and open-source intelligence to identify laundering patterns, coordinated networks, and shared infrastructure that would otherwise be difficult to discover manually.[58] When paired with blockchain analytics, these capabilities have already enabled law enforcement to trace illicit flows and recover assets tied to large-scale cryptocurrency fraud—outcomes that until recently were widely viewed as a near impossible feat to accomplish.[59]

Yet even as defenses adapt, the threat landscape continues to move. While stakeholders are still adjusting to AI-enabled techniques, the next wave of fraud and scams is already taking shape.[60] Agentic AI systems, for instance, are likely to introduce higher transaction volume and promise to shift more transactions to machine-to-machine execution, where intent, authorization, and accountability are harder to assess in real time.[61] At the same time, these technologies also expand what is possible for defenders. If deployed responsibly, agentic AI can support continuous monitoring, real-time risk assessment, and rapid intervention as transaction volume and velocity increase.[62] Quantum computing poses a longer-term challenge by threatening existing cryptographic safeguards, potentially lowering the cost of fraud if systems are unprepared, but it also holds promise for accelerating anomaly detection and pattern analysis across complex financial networks.[63] Ultimately, the impact of emerging technologies will depend

less on innovation itself than on policy choices that determine whether defenses can scale.

Moving Beyond the Crisis

Understanding how cybercriminals operate—who they are, how they think, and what makes them successful—should fundamentally shift how we respond. We cannot afford to treat these attacks as one-off crimes or blame victims for being targets.[64] We must recognize that financial fraud and scams are part of a larger system of exploitation, built on unchecked data flows, growing technological sophistication, and institutional blind spots.

While law enforcement and regulation remain essential, on their own they are not equipped to keep pace with the speed and scale at which today's cybercrimes evolve and occur.[65] Addressing this crisis effectively requires a whole-of-society approach, one that strengthens collaboration and coordination across sectors and embraces the role that emerging technologies can play in detecting suspicious activity early, tracing stolen funds, and protecting consumers in real time without distorting incentives or stifling innovative solutions.[66]

This shift in mindset matters. Combatting fraud and scams is no longer simply a consumer protection issue.[67] It is a fight for security, resilience, and trust in the digital age. Every American is now on the frontlines of the fight. Ensuring they are not left to face it alone is more than just good or pragmatic policy: it is a national security imperative. AA

Notes

1 Joe Vigil, "Las Vegas Vietnam Veteran Says He Lost $180,000 to Scammers," *Fox 5 Las Vegas*, December 26, 2024.
2 Jeffrey Gottfried et al., "Online Scams and Attacks in America Today," Pew Research Center, July 31, 2025.
3 Kevin Ozebek, "Scammers are Targeting Veterans at Alarming Rate. How to Protect the Vet in Your Life," ABC 7, June 3, 2025.
4 Matt Bracken, "House Bill Seeks to Better Tech to Combat Financial Fraud Scams against Elderly," *CyberScoop*, April 25, 2025.
5 Haiman Wong, "Cybersecurity Score – Guarding Unprotected Aging Retirees from Deception (GUARD) Act," R Street Institute, July 21, 2025.
6 "Fraud vs. Scams, Explained," PayPal, October 12, 2023.
7 PayPal, "Fraud vs. Scams, Explained."
8 "Social Engineering," Carnegie Mellon University, accessed February 2026.
9 "What to Know About Romance Scams," Federal Trade Commission, August 2022.

[10] "What are Some Common Types of Scams?," Consumer Financial Protection Bureau, March 13, 2024.
[11] "Arrest of the Confidence Man, *New-York Herald*, 1849," Lost Museum Archive, accessed February 2026.
[12] Lost Museum Archive, "Arrest of the Confidence Man, New-York Herald, 1849."
[13] Lost Museum Archive, "Arrest of the Confidence Man, New-York Herald, 1849."
[14] Toby Braun, "The Evolution of Fraud: New Platforms, Old Tricks," *Forbes*, August 26, 2024.
[15] Braun, "The Evolution of Fraud: New Platforms, Old Tricks."
[16] Braun, "The Evolution of Fraud: New Platforms, Old Tricks."
[17] Iyer, "Scams in the Digital Era: How Technology is Changing Fraud."
[18] Ugn Zienit , "Reconnaissance in Cybersecurity: Everything you Need to Know," NordVPN, December 30, 2024.
[19] Brian Joseph, "Advances in Financial Scam Tech Raises Alarms with State Legislators and Financial Sector," *LexisNexis*, August 31, 2023.
[20] Clara Fong and Abi McGowan, "How Myanmar Became a Global Center for Cyber Scams," Center on Foreign Relations, May 31, 2024.
[21] Fong and McGowan, "How Myanmar Became a Global Center for Cyber Scams."
[22] Fong and McGowan, "How Myanmar Became a Global Center for Cyber Scams."
[23] Fong and McGowan, "How Myanmar Became a Global Center for Cyber Scams."
[24] AJ Vicens, "Cybercrime Groups Offer Six-Figure Salaries, Bonuses, Paid Time off to Attract Talent on Dark Web," *CyberScoop*, January 30, 2023.
[25] Kate Fazzini, "Cybercrime Organizations Work Just Like Any Other Business: Here's What They Do Each Day," *CNBC*, May 5, 2019.
[26] Sheila Burke, "How Scammers Target Victims on Social Media," AARP, April 1, 2023.
[27] Paul Wagenseil, "Cybercrime, Inc.: How the Bad Guys Adopted the Business Model," *SC Media*, October 13, 2022.
[28] Alistair Simmons and Justin Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations," *Lawfare*, July 25, 2022.
[29] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."
[30] Simmons and Sherman, "Data Brokers, Elder Fraud, and Justice Department Investigations."
[31] Insikt Group, "The Business of Fraud: An Overview of How Cybercrime Gets Monetized," Recorded Future, February 25, 2021.
[32] Thomas Holt, "How Illicit Markets Fueled by Data Breaches Sell Your Personal Information to Criminals," Conversation, June 5, 2025.
[33] "Justice Department Announces Coordinated, Nationwide Actions to Combat North Korean Remote Information Technology Workers' Illicit Revenue Generation Schemes," U.S. Department of Justice, July 3, 2025.
[34] Google Threat Intelligence Group, "Cybercrime: A Multifaceted National Security Threat," Google Cloud, February 11, 2025.
[35] Jennifer Leach, "If Someone You Cared about Paid a Scammer, Here's How to Help," Federal Trade Commission, April 10, 2024.

[36] Leach, "If Someone You Cared about Paid a Scammer, Here's How to Help."
[37] Matt Alderton, "How and Where to Report Scams—and Why It's Crucial to Do So," AARP, December 29, 2025.
[38] Virginia Police Department, "Reporting Scams to Local Police: Understanding Their Role and Limits," AARP, July 2, 2025.
[39] NCSL Staff, "New Approaches in the Fight Against Consumer Fraudsters," National Conference of State Legislatures, November 11, 2025.
[40] "Fighting Fraud: Scams to Watch out For," Congress.gov, September 9, 2024.
[41] Alderton, "How and Where to Report Scams—and Why It's Crucial to Do So."
[42] Alderton, "How and Where to Report Scams—and Why It's Crucial to Do So."
[43] Alderton, "How and Where to Report Scams—and Why It's Crucial to Do So."
[44] Moya Crockett, "The Secret Health Hell of Being Scammed: 'I Felt as Though My Mind was Disintegrating'," *Guardian*, October 23, 2024.
[45] Caroline Melear, "Bipartisan Efforts are Underway to Tackle Financial Fraud and Scams," R Street Institute, July 17, 2025.
[46] Melear, "Bipartisan Efforts are Underway to Tackle Financial Fraud and Scams."
[47] Haiman Wong, "Cybersecurity Score – Guarding Unprotected Aging Retirees from Deception (GUARD) Act," R Street Institute, July 21, 2025.
[48] Wong, "Cybersecurity Score–Guarding Unprotected Aging Retirees from Deception (GUARD) Act."
[49] Brian Fritzsche, "Banks Are Fighting Fraud and Scams, But We Can't Do It Alone," Open Banker, July 10, 2025.
[50] "Bank Trade Groups Call out Misleading Warren Report on Zelle Fraud," ABA Banking Journal, October 3, 2022.
[51] Kennedy Meda, "Consumers or Financial Institutions: Who Bears the Burden of Scam-Induced Fraud Losses?," Thomson Reuters, August 13, 2024.
[52] Meda, "Consumers or Financial Institutions: Who Bears the Burden of Scam-Induced Fraud Losses?."
[53] Haiman Wong and Caroline Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI," R Street Institute, October 23, 2025.
[54] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[55] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[56] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[57] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[58] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[59] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."
[60] "Looking Ahead at the Future of Fraud," LexisNexis Real Solutions.
[61] Patrick Cooley, "How Agentic AI Could Turbocharge Fraud," Payments Dive, November 4, 2025.
[62] Haiman Wong and Tiffany Saade, "The Rise of AI Agents: Anticipating Cybersecurity Opportunities, Risks, and the Next Frontier," R Street Institute, May 29, 2025.

[63] Kate Whiting, "Quantum Leaps: 3 Ways Banks Can Harness Next-Gen Technologies for Financial Services," World Economic Forum, July 21, 2025.
[64] Meda, "Consumers or Financial Institutions: Who Bears the Burden of Scam-Induced Fraud Losses?."
[65] Mike Puglia, "Stop Blaming the Victim: Why the Fight Against Cybercrime Needs to Change," *Infosecurity Magazine,* July 4, 2025.
[66] Lindsey Johnson, "Sadly, the Scammers Are Winning—But Our Government Can Help," *Hill*, April 30, 2025.
[67] Wong and Melear, "Protecting Americans from Fraudsters and Scammers in the Age of AI."

This article originally appeared as an American Affairs *online exclusive, published February 20, 2026.*

Tyrants of the Algorithm: Big Tech's Corrosive Rule and Its Consequences

by Matt Stoller

REVIEW ESSAY

Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism

by Sarah Wynn-Williams

Macmillan, 2025, 382 pages

Back in early May, Facebook's chief of information security, Guy Rosen, was in court having to defend the indefensible. He was confronted with an email he had written seven years earlier, warning about the presence of groomers trying to sexually exploit children on Instagram. Facebook wasn't investing resources in addressing that rapidly growing problem. "Harmful Behavior . . . grooming especially," he wrote, "This really worries me given we're finding a lot of, umm, opportunity on FB, and given [Instagram]'s younger audience I bet we'll find we have work to do there."

A few minutes later, lawyers presented an even more explicit internal Facebook exhibit, titled "Inappropriate Interactions with Children on Instagram." During a three-month period in 2019, millions of minors were recommended by Instagram's algorithm to adults that Facebook had labeled "groomers," with frequent follow requests as a result. It was a detailed report showing how many recommendations occurred, how often they resulted in a follow request, and even showing a flow chart of the process. "We may be facilitating possible groomers finding young people," it added.

***Matt Stoller** is director of research at the American Economic Liberties Project and the author of* Goliath: The 100-Year War between Monopoly Power and Democracy *(Simon and Schuster, 2019).*

Here was evidence that one of the biggest companies in the world may have facilitated sexual predation of children on a massive scale, as if the Pizzagate scandal from QAnon were true, only done by Mark Zuckerberg. And yet, this shocking evidence got very little press attention. The Meta communications department did their job; they were able to cabin it to just *Bloomberg*, a trade publication called *MLex*, a Substack by Matt Taibbi, and a site I own called *Big Tech on Trial*.

What was perhaps even more surprising is that the judge in the case, James "Jeb" Boasberg, seemed annoyed by the exhibits. One would think that judges have some sort of moral compass and could at least be shocked. But this was an antitrust trial over Facebook's domination of social networking, and Boasberg, an older technocrat, just didn't see the relevance.

The basic claim by the government is that Facebook, in acquiring Instagram in 2012 and WhatsApp in 2014, was trying to thwart rivals from entering the social networking business that it monopolized. In most cases, a monopolist raises prices, and that's usually a big part of the record. But since Facebook doesn't charge explicit monetary prices to users, the plaintiff in the case, the Federal Trade Commission (FTC), took a different path, arguing that the quality of the product declined, in the form of a worse experience for users (i.e., more ads, more surveillance, and a less safe environment). The groomer evidence was put forward to show how Zuckerberg, after acquiring Instagram, didn't have to invest in the platform to make it safer, because there was no competition. Boasberg, however, pronounced the evidence "ancillary" to the case and expressed impatience with the FTC lawyers.

Twenty years ago, allegations that a large corporation was facilitating sexual predation of children would have been widely disseminated and the perpetrators punished, or at least noticed. But today, it goes largely unremarked, unnoticed. There have been dozens of scandals involving Facebook, everything from political censorship to a UN report accusing the firm of aiding genocide in Myanmar to Mark Zuckerberg offering to let Xi Jinping name his firstborn child. It's evident that Meta is a threat to American children, insofar as Zuckerberg was forced at a congressional hearing to apologize to the parents of kids exploited on the platform. It is also a threat to American national security, insofar as it has now been confirmed that Meta explicitly offered to help transfer technology to China so that nation could outcompete American firms.

But our political leadership class just cannot muster the energy or willpower to enforce any sort of moral or security order, and no one expects

laws to be anything but guidelines for the powerful. This is not surprising since Meta's reach extends to entrenched elites in both parties. Biden chief of staff Jeff Zients served on Meta's board of directors prior to his White House role; under Donald Trump, deputy chief of staff Steven Miller and Commerce Secretary Howard Lutnick are well-known and fierce allies of the firm. America is a very cynical place for a reason. It is also a profoundly weak nation, unable to answer the challenge from a powerful and ascendant Chinese state, or the crippling illegitimacy of failed internal governance going back to the George W. Bush administration. Our inability to do anything about Meta is a useful lens to understand why.

Oligarchy and Conscience Don't Mix

A company like Meta presents an interesting social question. What kind of corporation facilitates mass predation as a business model? And what kind of society tolerates this kind of behavior? At roughly the same time as the groomer exhibit came out, a former Facebook executive named Sarah Wynn-Williams gave us an answer, in the form of a gripping memoir of her time at the company. It's titled *Careless People: A Cautionary Tale of Power, Greed, and Lost Idealism,* which is a story of her time at Facebook from 2011 to 2017 helping the company navigate global diplomacy.

The book is named after the phrase in F. Scott Fitzgerald's classic novel *The Great Gatsby,* describing the piggishness of the idle wealthy class in 1920s America. "They were careless people," wrote Fitzgerald, "They smashed up things and creatures and then retreated back into their money or their vast carelessness, or whatever it was that kept them together, and let other people clean up the mess they had made." Suitably, the main theme of *Careless People* is wealth and neglect, with three main characters: Facebook founder Mark Zuckerberg; the company's Chief Operating Officer Sheryl Sandberg; and Republican consigliere Joel Kaplan, who was Wynn-Williams's boss for a large chunk of her time at Facebook.

There are many books on the misdeeds of Big Tech, but this one is only the second to treat the individuals at the heart of the great machine as human beings worthy of a novelist's eye. The other, *The Boy Kings: A Journey into the Heart of the Social Network* by Kate Losse, came out in 2012, long before Facebook was controversial, back when "making the world more open and connected" was taken seriously as a slogan. *Boy Kings* is a cult classic among people genuinely interested in the culture of Facebook, but it never gained widespread readership.

Careless People, by contrast, is a bestseller for a couple of reasons. The 2020s are very much like the 1920s, not just in the yawing differentials of power between the oligarchical class, then represented by the Rockefellers, Duponts, Mellons, and Morgans, but also because of the raw cynicism of the decade. The reforms of Barack Obama after a great financial crisis seemed a great ruse, just as Teddy Roosevelt's New Nationalism and Woodrow Wilson's New Freedom seemed a joke after the trauma of World War I. Hiram Johnson, one of the decade's leading progressives, noted that the people "are docile, and they will not recover from being so for many years." While it is not necessarily the case that Americans are docile today (though many of their political institutions and representatives evidently are), it is rational for ordinary citizens to turn away from stories like the one uncovered in the antitrust trial. After all, what's the point? No one's going to do anything about Facebook. Thus, Wynn-Williams, by presenting her story as a novel of corrupted fantastical wealth and power, is in touch with the moment.

The second reason the book is doing well is because Meta gave it a big publicity bump when the company threatened to sue the author if she did any interviews mentioning Meta, with the penalty of $50,000 every time she mentioned the company. The threat was a big news story, which propelled the book to bestseller status. Ironically, Meta's strategy has also worked: Wynn-Williams hasn't done a single interview since she was ordered to stay silent by an arbitrator. Facebook had publicly pledged in 2018 that it wouldn't rely on forced arbitration clauses, but like many such public statements, that was a lie. The "gag order was sought by a company whose CEO claims to be a champion of free speech," Wynn-Williams testified to Congress in one of her few public appearances. One result is that many of the lurid and important stories she discusses remain hidden in the pages of a book—because there's no one in the media promoting them.

And that's too bad because Wynn-Williams is an excellent storyteller, and *Careless People* is an important book. She chronicles the time when the company was morphing from a site for college kids to a dominant communications network that could influence elections and allegedly foster genocidal behavior. And she had a clear view of the top decision-makers in the company because her role was meaningful. She served as Facebook's chief diplomat, who helped Mark Zuckerberg and Sheryl Sandberg become global political icons, through the 2016 election.

The story starts with Wynn-Williams's childhood in New Zealand, where she survived a brutal shark attack and grew up to become an ideal-

istic activist, working on endangered species policy at the United Nations. It was there that she became obsessed with this new force in the world, social networking, which she concluded was going to become far more important than the bureaucratically stultifying structures of official world forums. Her instinct was reinforced when her hometown, Christchurch, was hit by an earthquake in 2011 while she was on the phone with her sister, who was trapped in the disaster, and the only place she could get information about whether her family survived was on Facebook. Facebook was the opportunity to actually change the world—if the company's leadership took the approach of building a responsible corporation.

Wynn-Williams pestered Facebook officials, unsuccessfully for months, about a job in the policy or political team. But she quickly encountered the cynicism of the company culture. "Facebook is this global political force that is going to change the internet and the world, and these things matter," she pleaded in one interview. "Matter to who?" came the response. "To the people who'll decide on rules that might stop Facebook from growing," she said, and that briefly got some attention. But Facebook is an American company, she was told, and they needed people who knew the FTC, Congress, and U.S. regulators who mattered. Even so, her comment that Facebook needed global diplomacy for business purposes would pan out, even if it showed a hint of darkness that belied her idealistic view of Facebook as a positive change agent.

Shortly after one of her interviews came the Arab Spring, and Facebook officials, mostly parochial technologists, politically connected Harvard graduates, and marketing specialists, were being told that Mark Zuckerberg should take credit for geopolitical events in the Middle East. They didn't know what to do, since taking credit for certain revolutionary movements in one part of the world could complicate their attempt to get into China. So, Wynn-Williams was brought on board, as "Manager of Global Public Policy," to build a diplomatic team and answer these kinds of questions. Still, as a naïve Kiwi with an idealistic take on what Facebook could do for the world, she was an outsider within the company.

Wynn-Williams presents her story as a witness to the corruption of Facebook, arguing that when she first arrived, the company was vibrant, fun, and joyful. "There was a boisterous, happy energy to the place," she wrote. Soon after she arrived, politicians began to drop by Facebook to meet with Zuckerberg, who was a growing celebrity, but one who loathed politics and was interested purely in technology and power. By contrast, Sandberg was an immensely talented politician herself. In the first visit

by a foreign political leader to Facebook, New Zealand Prime Minister John Key reached out to Zuckerberg's hand to shake it, but the tech mogul "looked stricken and jumped back," irritated and uncomfortable. By contrast, Sandberg, in her element, "transformed from a normal-looking fortysomething woman into someone genuinely glamorous . . . her hair, her eyes, her makeup, her skin—suddenly she positively glows."

Still, even at first, Wynn-Williams noticed a Gatsby-esque environment of luscious entitlement. There was so much money at the company, it was almost inconceivable. She got "distracted in meetings by women's engagement rings that are so large it looks like it's hard for them to type, and diamond bracelets that cast small rainbows on the wall and clatter against laptops." The office was like a "never-ending kid's birthday party. All meals are provided, endless free snacks, game arcades. Bring your laundry to work and someone will do it for you." There were employees who called themselves "ex-Googler volunteers," meaning they had come over from Google with so much money that their salaries at Facebook were irrelevant; they were just there for the stock options.

Facebook's Unholy Trinity

In 2013, at the height of the Obama era, Sandberg published *Lean In: Women, Work, and the Will to Lead*, moving from chief operating officer to celebrity. And Wynn-Williams started seeing another side of the company and the people who ran it. After Wynn-Williams came back from maternity leave, Sandberg gave her some advice: "Be smart and hire a Filipina nanny," she said. "They're English speaking, sunny disposition, and service orientated." Wynn-Williams soon noticed that both of Sandberg's key advisors had Filipina nannies as servants.

Sandberg was gradually revealed as a narcissistic bully with a pathological need for attention who regularly harassed subordinates. When Wynn-Williams complained that Sandberg tried to coerce her into bed on a private jet, she was told "'half the department' has been in Sheryl's bed by now." Sandberg lavished favors on those who did her bidding and iced out those who didn't. She spent thousands of dollars on lingerie for an assistant, Sadie, known as Sheryl's "little doll."

At certain points, Sandberg's behavior veered into the downright bizarre. She hated using Facebook, and yet after returning from Japan on one occasion, she posted that she was nearly booked on a commercial flight that crashed, which just wasn't true. "People don't lie about narrow-

ly missing plane crashes, do they?" Wynn-Williams writes. "Why would she? It's not like she needs attention."

As Facebook became more powerful and globally influential, Wynn-Williams took on increasing responsibility to make the firm look good. This attempt took two forms. The first was fake do-gooder nonsense. Sandberg, for instance, wanted the company to push charitable causes, with predictably disastrous results when she sought to use Facebook to encourage organ donations worldwide, despite different ethics and laws in every country. Another example was a cynical and failed attempt to provide cheap internet to poor countries, which was actually about locking in more Facebook users.

The second was to manipulate political leaders who might otherwise seek to regulate or tax the company. The company developed a method to manipulate skeptical politicians, with the growth team saying they would "juice" the algorithm to grow their Facebook presence. "Let's dial up the algorithm to give politicians some love," was the internal expression. Wynn-Williams was constantly surprised that the more abrasive Facebook was, the more success they had; politicians, far from upset, became putty in Zuckerberg's hands.

Zuckerberg himself went through a transformation as well, turning from a largely apolitical technologist into a political figure with megalomaniacal ambitions. He, too, was surrounded by sycophants constantly praising his decision-making, amplifying his worst impulses, and doing petty, pathetic things like letting him win at *Settlers of Catan.* An inflection point for Zuckerberg was the 2016 election, after Facebook had poured immense resources into helping the Trump team run a remarkable advertising campaign. Internally, they called it the "Facebook election." No one seemed to care that they were putting their thumb on the scale for Trump, since Kaplan and Sandberg found it inconceivable that Trump would win. But then, he did.

Zuckerberg at first refused to concede that Facebook had anything to do with Trump's win, saying the "idea that that had any impact in the election is pretty out there." Eventually, though, he began to understand that every politician saw him as a kingmaker. And yet his newfound power, which Wynn-Williams thought might foster a sense of responsibility, only made him less interested in it.

Eventually, Zuckerberg became openly thuggish, demanding that his team adopt the "street fighter tactics" that Uber uses, such as strikes and protests, as well as opposition research on journalists. He demanded lists

of adversaries and that his team figure out "ways to use the platform and the algorithm to pressure them. He wants to establish a team within Facebook to figure out how to build the tools that will use the algorithm and platform to pressure adversaries, including politicians who oppose us, to bolster the policy team." Who is an adversary, she asked. "Anyone who opposes us is an adversary," he said. Finally, in a fit of megalomania, he noted that newspapers were all dying and mused on replacing the entire media with something on Facebook, what he called the "Fifth Estate."

The third major character is Joel Kaplan, a George W. Bush–era operative who helped bring Facebook closer to the Trump administration. Kaplan was "Sheryl's ex-boyfriend," part of a "a web of people all entangled as bridesmaids, best friends, neighbors, and exes," who comprised the firm's leadership team. Kaplan also seemed particularly uninterested in the world, surprised at one point to learn that Taiwan is an island. "Often when we start to talk about pressing issues in some country in Latin America or Asia, he stops and asks me to explain where the country is."

As Facebook's diplomatic endeavors became more important, Wynn-Williams was forced to take responsibility for the company's expansion in Myanmar, as well as its aborted attempt to get into China. Myanmar was a strange country for Facebook to prioritize, but at the time, Zuckerberg was obsessed with network effects: the more users, the more dominant Facebook would be. So, any and every large population needed to be on Facebook, no matter how poor. The company entered Myanmar just as people got access to the internet; for most citizens, Facebook itself was the internet. And Facebook in Myanmar, with little civil society infrastructure after decades of military rule, was particularly susceptible to manipulation. After ensuring that the population was using Facebook, no one at Facebook paid attention to how they used it.

Soon, Wynn-Williams's team, as well as human rights groups, uncovered significant evidence to show that the company's entrance into Myanmar—and its refusal to do any meaningful investment in the country—might have been leading to a gruesome outcome: the military junta fostering a genocide against the country's Muslim population, allegedly using Facebook as a key organizing vehicle. The military would do things like hack into the accounts of celebrities and spread false stories of rapes by Muslims. But it didn't matter how much information Wynn-Williams presented to prove that the firm had a substantial role in this catastrophe: corporate decision-makers didn't act, and the genocide continued, with Facebook as an alleged enabler.

"Myanmar would've been far better off if Facebook had never arrived there," she noted. "I've spent a lot of time thinking about what unfolded next in Myanmar, and Facebook's complicity. It wasn't because of some grander vision or any malevolence toward Muslims in the country. Nor a lack of money. My conclusion: It was just that Joel, Elliot, Sheryl, and Mark didn't give a fuck."

And always, there was money, endless amounts of money and the things that money bought: private jets; rare, endangered tuna costing tens of thousands of dollars; and lavish tropical settings for the senior team, all of which contrasted with a creepy authoritarian vibe for those considered unimportant. There were also routine and unthinkably cruel moments happening at Facebook itself. Executives did not seem to care if Facebook employees were sent to prison for the company's policies.

At one point after the 2016 election, Wynn-Williams witnessed a woman in a Facebook open office space convulsing on the floor and foaming at the mouth, with her face bleeding. Everyone was ignoring her, "busily typing on their keyboards." Wynn-Williams tried to get some basic information from the people around the woman, so she could call 911 and give them her name and possible medical condition. She asked a person at a nearby desk if she is her manager. "Yes," she snapped. "But I'm very busy." Besides, "she's a contractor [and] her contract's coming to an end soon. I suggest you call HR." The woman continued foaming at the mouth.

"The idea that someone could be in pain, writhing at your feet, and just be ignored, that was unthinkable," Wynn-Williams wrote. This cruelty came for Wynn-Williams herself and ultimately led to her dismissal. Toward the end of her time at Facebook, she nearly died, ending up in a coma after a particularly difficult childbirth. Kaplan, who was her boss, decided to give her a performance review after she came back from maternity leave. "You weren't responsive enough," he told her. "In my defense," she responded, "I was in a coma for some of it."

Kaplan himself sexually harassed Wynn-Williams, frequently and disturbingly. When she tried to tell him she can't go to India because she is trying not to wean her daughter, he demanded an in-depth explanation of breastfeeding. And then there's this, the following passage is honestly one of the most disturbing parts of the book:

> On one of our regular video calls during my maternity leave, he asks me how my health is. I keep my answer brisk and professional: I'm still very sick, I'm going to need more surgery. "But where

> are you bleeding from?" he asks. My mind races. There is no way he doesn't know. "Seriously? Um, well, it's the same place I've been losing blood from all along." "What place?" he presses, insistent. "Do we have to go into this?" He stares me down from his bed, propped up by voluminous pillows, and asks again about where the blood is coming from. "I'm not really comfortable." "Come on, Sarah," he pushes. "Well, it's not my eyes . . . ." He starts to get angry. "I have to go."

Sexual harassment is a big theme at Facebook, with hundreds of women secretly organizing around the problem, as Zuckerberg's righthand man, Elliot Schrage, orchestrated coverups for powerful men like Kaplan.

Throughout the book are layered the political and policy scandals about which we are aware, such as Facebook pitching advertisers on how to target teenage girls when they feel "worthless," "insecure," "stressed," "defeated," "anxious," "stupid," "useless," and "like a failure." The company issued a statement: "Facebook does not offer tools to target people based on their emotional state," which was a "flat-out lie," according to Wynn-Williams.

Truth and Reckoning

As I was reading this book, I had a hard time believing these stories were true. And yet, they most likely are, because Meta has a brutal legal department and would litigate against her for defamation if they weren't. I asked a college classmate who worked at Facebook at the time about Mark Zuckerberg, whom he found charming and intelligent. Would it make sense for Zuckerberg to be so open about wanting to rule the world? "Oh, that. Yeah, Mark's a little bit of a megalomaniac." Americans have lost faith, broadly speaking, in our institutions, but this book made me wonder if we're really cynical enough. One critique of the book is that Wynn-Williams has a sort of liberal gloss on her politics and that diminishes her political analysis. But not by much.

And that brings me back to why this book, despite being a bestseller, has had such a limited political impact so far. The author is under a gag order. Aside from one podcast, at the time of this writing, the only public commentary Wynn-Williams has made about this book was when she testified before the Senate Judiciary Subcommittee on Crime and Counterterrorism on the company's foreign policy choices, at the invita-

tion of Big Tech scourge, Republican Senator Josh Hawley. That hearing was titled *A Time for Truth: Oversight of Meta's Foreign Relations and Representations to the United States Congress.* Here are some of the revelations from that hearing that were also in the book:

Facebook had a secret mission to get into China called "Project Aldrin" that was restricted to "need-to-know" staff. Wynn-Williams "witnessed Meta work 'hand in glove' with the Chinese Communist Party to construct and test custom-built censorship tools. . . . When Beijing demanded that Facebook delete the account of a prominent Chinese dissident living on American soil, they did it. And then lied to Congress when asked about the incident in a Senate hearing."

The company provided the Chinese government access to the user data of Americans. It also built a physical pipeline connecting the United States and China, despite "warnings that this would provide backdoor access to the Chinese Communist Party, allowing them to intercept the personal data and private messages of American citizens." Congress blocked the pipeline. Facebook actively and explicitly sought to help Chinese companies outcompete U.S. firms by "providing technological expertise on critical issues such as data center networking equipment, general purpose and GPU servers, storage devices and appliances, and scalable rack designs" to Chinese experts.

Facebook has also lost its edge in being able to develop and deploy innovative products. Failures include: "the Facebook phone, Internet.org, Building 8, Facebook Portal, Workplace, it's crypto product-Diem/Libra, Moments, Flash, Meta Spark, Rooms, Facebook News, Parse, Open graph, Aquila, Facebook gifts, Places, Riff, Bonfire, Slingshot, Facebook Questions, Satellites, Credits, Creative Labs, Cambria, Horizon Home, Horizon World and the Metaverse."

After watching that hearing, listening to the antitrust case, and reading this book, I have come to what amounts to a pretty obvious conclusion: Facebook is a deeply disturbing firm run by terrible human beings. Wynn-Williams's book has simply confirmed with its vivid, disturbing details what many could already see and suspect: it is destroying America and tearing apart its social fabric, and it is doing the same to every other society that has let it run loose. I realize that's not a very nuanced or interesting conclusion, but sometimes the obvious point is all there is. But that leads us to the more important question. Why do we permit Meta to exist in its current form?

Meta isn't some despotic force that suddenly descended on the United States; it is an advertising firm whose activities are rooted in a legal framework that allows and encourages extractive behavior. The rationale for Meta's existence in its current form is simple, but it's not one that would be recognized as a counterargument to the scandals laid bare over many years.

America's Highest Values

On CNBC, hype man Jim Cramer can frequently be seen lauding Meta and Mark Zuckerberg for delivering knockout investor returns, dismissing any and all scandals, and claiming that the firm is generally just great for America. Zuckerberg's new strategy, he notes, is about disrupting all advertising with generative artificial intelligence: just have corporations connect their bank accounts with Meta and give it a business objective, and the social media giant will use its new AI-infused technology to make an ad campaign and run it without any other input.

Cramer even coined a term, "MNM," for high-performing stocks; it is named for Microsoft, Nvidia, and Meta, all multitrillion-dollar firms whose basic businesses sit at the nexus of market power and large computing resources. To that end, Zuckerberg, after his latest failure to sufficiently advance his firm's high-end large language model Llama, is now throwing around paychecks of nine figures to attract data scientists from rival firms. For Zuckerberg, objectives like stopping Instagram's algorithm from sending groomers to children, or preventing a genocide in Myanmar, should have zero resources; but to win at AI, which is to say, to secure dominance in information management, money is no object.

Such an argument shouldn't be dismissed out of hand because it is a moral claim. Cramer's view, and likely Zuckerberg's, is that scandalous behaviors and policies like all the ones laid out by Wynn-Williams might suggest harm, but they might not. They are, in any case, the wrong metric for success. Claims of unfairness or human harm are flabby and arbitrary, unlike the cold hard numbers of the equity markets which reveal efficiency at work. Cramer's view is essentially a distillation and proof of the argument in Julius Krein's 2021 *American Affairs* article titled "The Value of Nothing: Capital versus Growth," in which Krein noted that the "U.S. economy is, to a unique extent, organized around maximizing asset values and returns on capital independently of growth—in terms

of corporate behavior, financial market incentives, and government and central bank policy."

A different way to put it is Joe Weisenthal's argument that America's social system requires men like Zuckerberg, who has certainly created market capitalization for investors. "A stock market that continues to go up is part of the entire US economic model," Weisenthal wrote. "Rising stocks are how we pay for retirement, education, consumption, and so forth . . . any impulse to abundantly build out less profitable lines of business undoubtedly strikes at the heart of how American capitalism works." Zuckerberg is unbounded because the stock market must go up; he is where he is because maintaining high asset values is now America's highest value.

If Zuckerberg didn't try to sell out America to China, or if he genuinely tried to do something about the myriad ethics allegations leveled against him, he would never have been CEO of Facebook in the first place. By contrast, China's stock market hasn't risen in fifteen years, which is why that country is not only capable of regulating social media, but also governing in a variety of ways now foreclosed to America: Beijing has used a production model based on high volume and low margins for real, physical goods to become the workshop of the world. Building rare earth magnets isn't particularly hard or expensive for an immensely wealthy nation like the United States, just as putting together a few tools to prevent crimes against humanity or the exploitation of minors wouldn't have been tough for a company like Facebook. But seeing risk or social problems outside of equity values just isn't how we do things in America these days.

That might be why, despite Joe Biden's active dislike of Mark Zuckerberg and bipartisan calls to repeal the liability shield for big tech firms known as Section 230, Meta has consistently flourished as a corporate entity. The Kids Online Safety Act was an attempt to regulate the most basic parts of social media, notably the surveillance of underaged users; it passed the Senate in a 91-3 vote in 2024. It even had the support of Elon Musk. Yet it ultimately floundered as Meta allies Steve Scalise and Mike Johnson blocked it in the House, due to big tech money and influence. More broadly, this theme, of the failure of even the easiest possible legislative lifts for obvious problems—such as reform of the convoluted way we buy pharmaceuticals through third-party PBMs, or the need to regulate railroads to prevent explosions like we saw in East Palestine, Ohio—is consistent. We must sacrifice our wellbeing, national

security, global bargaining position vis-à-vis China, and the safety of our children, so that the stock market can go up.

In the beginning of Trump's second term, we saw what might have been something different. From January to early May, the administration announced a variety of tariffs, and equity markets fell. Far from concerned, Trump seemed almost pleased at the broad-based freakout by Wall Street, which had been excited for an administration planning to cut corporate taxes and get rid of green energy initiatives. "Sometimes you have to take medicine to fix something," Trump said. Had he continued to ignore the pleadings of capital market actors, he could have (in his own strange and inexplicable way) freed America from the rule of men like Zuckerberg. This is because our need for their harsh existence is based on prioritizing a high return on capital over all other social values. Smash that, and you open the door to something new.

But Trump didn't. Instead, like every president before him since Ronald Reagan, he hewed to the famous dictum of political strategist James Carville, who described why Bill Clinton abandoned his populist pledges in the 1990s. "I used to think that if there was reincarnation, I wanted to come back as the President or the Pope or as a .400 baseball hitter," Carville said. "But now I would want to come back as the bond market. You can intimidate everybody." After mostly retreating on tariffs, especially the ones initially imposed on China, the stock market came roaring back, to Trump's delight. No longer would Wall Street be "yippy" under his watch.

And so, Trump, encouraged by Lutnick and Miller, is actively and aggressively seeking to boost Mark Zuckerberg's power. His trade agenda is focused not on restoring U.S. manufacturing but making sure that Europe withdraws its Digital Markets Act, that Canada and India stop trying to tax Big Tech, and that South Korea repeal its antimonopoly laws applying to firms like Meta. He ensured that Meta could hire through the controversial H-1B visa program, which allows for American corporations to bring in low-wage immigrant labor, often for information technology jobs. And unlike in his first term, his agenda will likely allow Meta to launch its own stablecoin currency. Even with the antitrust case, which is ongoing, Trump was sorely tempted to settle it for a paltry sum, though was talked out of it by advisers.

In other words, as ugly a story as Mark Zuckerberg and Meta might be, that's far less bad than the weakness of America in enabling it. In any sane nation, this company would not exist in its current form, and

Mark Zuckerberg would probably be in handcuffs for what he's done in pursuit of unbridled power; the abuses exposed by Wynn-Williams and others would be fuel for a political revolt and candidates would be competing to prove who could best fight back against Meta—instead of who could best serve it. Yet nothing is likely to change until such a time when Americans, or really any other nation, can truly wake up from this long period of docility and assert the need for bold, systemic reform, and that's what we should endeavor to make happen. AA

This article originally appeared in American Affairs *Volume IX, Number 3 (Fall 2025): 85–98.*