Duquesne Law Review

Volume 59 | Number 2 Article 5

2021

Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked

April Falcon Doss

Data Privacy & National Security: A Rubik's Cube of Challenges and Opportunities That Are Inextricably Linked

April Falcon Doss[*]

I. INTRODUCTION 232
II. "CYLINDERS OF EXCELLENCE": VIEWING DATA-RELATED ISSUES THROUGH DIFFERENT LENSES OF LAW 233
III. UNDERSTANDING HOW THE SAME PERSONAL DATA CREATES RISKS FOR INDIVIDUAL PRIVACY AND FOR NATIONAL SECURITY 236
IV. PRIVACY AND NATIONAL SECURITY ARE NOT ALL: THE INTERSECTIONS AMONG DEPLATFORMING, CONTENT MODERATION, ANTITRUST, AND ONLINE HARMS 251
V. LESSONS IN OVERSIGHT—AND HOW TO IMPROVE PRIVACY AND DATA PROTECTIONS WHILE ALLOWING REASONABLE GOVERNMENT USE 256
VI. HOW CAN, OR SHOULD, THESE AREAS OF LAW INTERSECT? 261
A. Acknowledge the Convergence of Technology—and Embrace Cross-Pollination of Legal Theories 263
B. Expand Data-Related Regulations on the Private Sector 264
C. Level the Playing Field in Government Regulations 264
D. Prioritize Education and Public Awareness Campaigns 265
E. Empower Congressional Oversight with Cross-Committee Jurisdiction 266

* April Falcon Doss is Executive Director for the Georgetown Institute for Technology Law & Policy at the Georgetown University Law Center. Prior to that, she chaired the cybersecurity and privacy practice of a major U.S. law firm, served as Senior Minority Counsel for the Russia Investigation in the United States Senate Select Committee on Intelligence, and spent over a decade at the National Security Agency, where she was Associate General Counsel for Intelligence Law.

F. Assess the Need for Additional Independent Oversight Bodies.....266
VII. CONCLUSION.....267

I. INTRODUCTION

Traditionally, issues relating to information privacy have been viewed in a set of distinct, and not always helpful, stovepipes—or, as my former government colleagues often said, tongue-in-cheek, in other contexts—separate "cylinders of excellence." Thanks to the convergence of technologies and information, the once-separate realms of personal data privacy, consumer protection, and national security are increasingly interconnected. As Congress and national policymakers consider proposals for federal data privacy legislation, regulation of social media platforms, and how to prevent abuses of foreign intelligence and homeland security powers, they should be examining each of these challenges in light of the others, actively looking for synergies and overlap in the protections they may be considering for protection of personal data, individual privacy, and civil liberties.[1]

1. It should be noted that this need for cross-pollination of issues and approaches is not limited to the United States. The European Union has, for some years, taken a stove-piped view of data protection in the EU, while examining data privacy in the U.S. through a converged view that blends the commercial context of cross-border data transfers with government-directed national security activities. This difference in approach has resulted in the European insistence that commercial transactions between U.S. and European entities be subject to heightened protections for cross-border data flows because of EU objections to U.S. foreign intelligence activities, despite the fact that a great deal of U.S. intelligence analysis is shared with allied European governments. These concerns have been apparent in the establishment of restrictions on cross-border data flows under the Data Protection Directive and European negotiation of the Safe Harbor data transfer scheme with the U.S.; the collapse of the Safe Harbor regime following revelations about U.S. surveillance programs; the enactment of new cross-border data transfer restrictions under the General Data Protection Regulation; the establishment of the new Privacy Shield mechanism for cross-border transfers; and the invalidation of Privacy Shield under the *Schrems II* decision of the Court of Justice of the European Union in the summer of 2020. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, 2020 E.C.R. I-559. The dissonance between European approaches to internal and external legal regimes stems from the fact that the EU lacks competence over national security programs of its member nations—positioning the EU to criticize the U.S. without having to undertake similarly close examination of surveillance programs of EU nations, even where those programs may be similarly intrusive and less transparent. As a result, the cross-border data transfer restrictions of the GDPR are at risk of functioning more as a market protection mechanism, forcing data localization in the EU that redounds to the commercial benefit of EU-based technology platform companies, without meaningfully increasing the privacy protections of EU residents, who remain subject to surveillance pursuant to the national authorities of the member nations of the European Economic Area, where their data may be freely transported without restriction and largely without review of national security, domestic security, or other government uses of personal data.

II. "CYLINDERS OF EXCELLENCE": VIEWING DATA-RELATED ISSUES THROUGH DIFFERENT LENSES OF LAW

Historically, information privacy in the U.S. has been governed through a series of separate legal frameworks that sometimes run parallel to each other with little overlap, and other times align in ways that are orthogonal to each other. The approaches to personal information protection in the consumer privacy and national security contexts have followed largely separate paths, while the expansive territory of consumer data protection includes examples of a number of different approaches that sit, conceptually, at right angles to each other.

Consumer privacy as a whole has been regulated as a somewhat amorphous, or at least variable, concept, with different jurisdictions taking different approaches to different kinds of information, some providing only for regulatory enforcement,[2] while others support statutory damages and a private right of action.[3] One set of approaches can best be described as a mile wide but an inch deep: the classic example of this is state data breach laws, which generally aim to protect all residents in a jurisdiction and impose notification obligations on most organizations that holding those individuals' information; but those laws only cover a narrowly defined set of information, generally focused on government-issued identification numbers and financial account information.[4] In recent years, a growing number of states have enacted laws extending some rights

---

See, e.g., APRIL FALCON DOSS, CYBER PRIVACY: WHO HAS YOUR DATA AND WHY YOU SHOULD CARE 242–46 (2020).

2. For examples of federal privacy-related statutes that include regulatory enforcement mechanisms but do not support a private right of action, *see, e.g.*, Federal Trade Commission (FTC) Act, 15 U.S.C. § 45; Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506; Graham-Leach-Bliley Act (GLBA), 15 U.S.C. §§ 6821–6827; Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in 42 U.S.C. § 1320d-6).

3. For examples of federal privacy-related statutes that support a private right of action, *see, e.g.*, Privacy Act, 5 U.S.C. § 552; Fair Credit Reporting Act, 15 U.S.C. § 1681p; Video Privacy Protection Act, 18 U.S.C. § 2710(c); Telephone Consumer Protection Act, 47 U.S.C. § 227(b)(3). For examples of state privacy laws that include a private right of action, *see, e.g.*, California Consumer Privacy Act of 2018 (CCPA), CAL. CIV. CODE §§ 1798.100–1798.199; Illinois Biometric Information Privacy Act (BIPA), 740 ILL. COMP. STAT. ANN. 14/5.

4. All fifty states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation that requires the government or private entities to inform consumers of data breaches that involve personally identifiable information. *Security Breach Notification Laws*, NAT'L CONF. STATE LEGIS. (July 17, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

and obligations to biometric information[5] and the sweeping California Consumer Privacy Act (CCPA),[6] and the amendments passed by ballot referendum as the California Privacy Rights Act, which expanded consumer rights and company obligations with respect to personal data in a number of significant ways.[7] At the federal level, consumer privacy was regulated by the Federal Trade Commission (FTC) under Section 5 of the Federal Trade Commission Act's prohibition on unfair and deceptive acts and practices.[8] The FTC has regulated a series of privacy-related laws governing specific areas of information privacy, ranging from laws intended to protect specific groups, like the Children's Online Privacy Protection Act (COPPA),[9] to laws aimed at regulating specific industries, like the Graham-Leach-Bliley Act (GLBA)[10] regulation of the financial services industry. Employment privacy has generally been left unaddressed by federal statute,[11] while a specific, and somewhat narrow, slice of health-related privacy has been governed by the Health Insurance Portability and Accountability Act (HIPAA)[12] and HiTECH Act,[13] regulated and enforced by the Department of Health and Human Services' (DHHS) Office of Civil Rights (OCR), and a similarly specific, and somewhat narrow, side of education-related information has been subject to privacy protections under the Family Education Rights and Privacy Act (FERPA),[14] administered by the Department of Education.

Meanwhile, use of information for national security, homeland security, and law enforcement purposes has been underpinned by the Fourth Amendment to the Constitution and further regulated by a host of statutes, including the Foreign Intelligence Surveillance Act (FISA),[15] Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism Act of

5. *See* CAL. CIV. CODE §§ 1798.100–1798.199; 740 ILL. COMP. STAT. ANN. 14/5; LA. STAT. ANN. §§ 51:3071–51:3077; N.Y. GEN. BUS. LAW § 899-bb; OR. REV. STAT. §§ 646A.600–646A.628.

6. CCPA §§ 1798.100–1798.199.

7. The California Privacy Rights Act was passed as Proposition 24 on the November 2020 ballot and amends key provisions of CCPA. *Id.*

8. 15 U.S.C. § 45.

9. 15 U.S.C. §§ 6501–6506.

10. 15 U.S.C. §§ 6821–6827.

11. Bradley A. Areheart & Jessica L. Roberts, *GINA, Big Data, and the Future of Employee Privacy*, 128 YALE L.J. 710, 761 (2019).

12. 42 U.S.C. § 1320d-6.

13. Pub. L. No. 111-5, 123 Stat. 115 (codified at 42 U.S.C. § 300jj–300jj-51).

14. 20 U.S.C. § 1232g.

15. 50 U.S.C. §§ 1801–1813.

2001 (USA PATRIOT Act),[16] USA Freedom Act,[17] the Electronic Communications Privacy Act (ECPA),[18] the Wiretap Act,[19] the Stored Communications Act (SCA),[20] and Executive Orders, including Executive Order (EO) 12333, and federal and state laws on computer crimes, including the Computer Fraud and Abuse Act (CFAA) and similar state laws.[21]

At first blush, this separate treatment of consumer data protection and privacy in national security not only makes historical sense but appears reasonable today as well. After all, government action is appropriately subject to Constitutional constraints, including the First and Fourth Amendments, while private action by commercial or other nongovernmental actors is generally not subject to those constraints. Action by the government can have more dire consequences to civil rights and civil liberties, as one recent commenter posted on social media[22]:

For all these reasons and more, perhaps it is no wonder that recent news articles have sounded a note of alarm in their coverage of programs under which the U.S. intelligence community is allegedly purchasing commercially available information from data brokers who amass detailed personal profiles on individuals based on their

16. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (amending provisions throughout sections of the U.S. Code, such as at 50 U.S.C. § 1861(a)(1)).

17. Pub. L. No. 114-23, 129 Stat. 268 (codified as amended in 50 U.S.C. 1881a).

18. 18 U.S.C. §§ 2510–2522, 2701–2711, 3121–3127.

19. 18 U.S.C. §§ 2510–2522.

20. 18 U.S.C. §§ 2701–2711.

21. *See* 18 U.S.C. § 1030; *see also Computer Crime Statutes*, NAT'L CONF. STATE LEGIS. (Feb. 24, 2020), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (providing a state by state breakdown of computer crimes statutes).

22. @SaysMyDerbyWife, TWITTER (Jan. 22, 2021, 1:41 PM), https://twitter.com/SaysMyDerbyWife/status/1352687762999300102.

usage of mobile phone apps.[23] Although information from cell phone apps is widely available for purchase as part of the multi-billion-dollar advertising technology, or adtech, industry,[24] the idea of its use by government officials raises any number of concerns about a possible dystopian surveillance state.

A different way of understanding these issues, however, is to look at the growing number of events in recent years in which technology and information have intersected in ways that impact individuals, geopolitics, and national and domestic security risks, and to conclude that this convergence of facts argues in favor of greater integration of legal and policy approaches as well. Viewed in that light, the news reports about the U.S. Intelligence Community (USIC) purchasing commercially available information can be seen not so much as a threat to traditional Fourth Amendment legal theory, but instead as an opportunity to holistically assess what rights, obligations, and remedies should be imposed under a cross-functional legal theory that tries to balance legitimate government aims with reasonable consumer protections and formulate a predictable set of boundaries, guardrails, and constraints.

III. UNDERSTANDING HOW THE SAME PERSONAL DATA CREATES RISKS FOR INDIVIDUAL PRIVACY AND FOR NATIONAL SECURITY

Over the past five years, a series of events have underscored the ways in which personal information and social media platforms, can be used to heighten geopolitical tensions, increase national security risk, and—to borrow a phrase from the nation's founders—threaten domestic tranquility. The most obvious categories are election security, cybersecurity threats, foreign counterintelligence operations, and domestic terrorism and insurrection, each of which is summarized with brief highlights from recent events, below.

First, election security. The Russian government's interference with the 2016 U.S. presidential election has been well documented.

---

23. *See, e.g.*, Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES, https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html (Jan. 25, 2021); Byron Tau, *Military Intelligence Agency Says It Monitored U.S. Cellphone Movements Without Warrant*, WALL ST. J. (Jan. 22, 2021, 4:19 PM), https://www.wsj.com/articles/military-intelligence-agency-says-it-monitored-u-s-cellphone-movements-without-warrant-11611350374.

24. *See, e.g.*, *Mobile Advertising Market Size, Share & Industry Analysis, by Advertising Type (In-App Ads, Mobile Rich Media, Video Ads, Banner Ads, Others), by Vertical (Retail, Media & Entertainment, Healthcare, BFSI, E-Commerce, Travel & Tourism, Automotive, Others), and Regional Forecast, 2019–2026*, FORTUNE BUS. INSIGHTS (Mar. 2020), https://www.fortunebusinessinsights.com/mobile-advertising-market-102496.

The Senate Select Committee on Intelligence (SSCI) conducted a lengthy investigation into the Russian active measures campaign, an investigation that included dozens of witness interviews, review of thousands of pages of documents, open and closed hearings, and that resulted in a lengthy, five-volume report.[25] Among other conclusions, the Senate report noted:

> [i]n 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency (IRA) used social media to conduct an information warfare campaign designed to spread disinformation and societal division in the United States. . . . Masquerading as Americans, these operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with and attempt to deceive tens of millions of social media users in the United States. This campaign sought to polarize Americans on the basis of societal, ideological, and racial differences, provoked real world events, and was part of a foreign government's covert support of Russia's favored candidate in the U.S. presidential election.[26]

One key to the Russian information operation: personal data of Americans. In testimony before the Senate Judiciary Committee, Christopher Wylie, the former research director of the political consulting firm Cambridge Analytica and UK defense contractor SCL Group, described the ways in which detailed personal information about individual Facebook users was leveraged by Cambridge Analytica (CA) as part of a set of information operations intended to influence the 2016 presidential campaign. Wylie explained how SCL Group created CA with funding from American billionaire Robert Mercer, installing political operative Steve Bannon as one of CA's senior officers "to build an arsenal of informational weapons he could deploy on the American population."[27] Wylie emphasized in his written testimony that:

> [t]he purpose . . . was to develop and scale psychological profiling algorithms for use in American political campaigns. To be clear, the work of CA and SCL is not equivalent to traditional

25. *See generally* S. REP. NO. 116-290 (2020).

26. 2 S. REP. NO. 116-290, at 3 (2020).

27. *In the Matter of Cambridge Analytica and Other Related Issues: Written Statement to the U.S. S. Comm. on the Judiciary*, 115th Cong. 2 (2018) (testimony of Christopher Wylie, former Research Director, Cambridge Analytica) (available at https://www.judiciary.senate.gov/imo/media/doc/05-16-18%20Wylie%20Testimony.pdf) [hereinafter Testimony of Christopher Wylie].

> marketing, as has been claimed by some. This false equivalence is misleading. CA [specialized] in disinformation, spreading [rumors], kompromat and propaganda. Using machine learning algorithms, CA worked on moving these tactics beyond its operations in Africa or Asia and into American cyberspace.[28]

Specifically, Mr. Wylie noted:

> CA sought to identify mental and emotional vulnerabilities in certain subsets of the American population and worked to exploit those vulnerabilities by targeting information designed to activate some of the worst characteristics in people, such as neuroticism, paranoia and racial biases. This was targeted at narrow segments of the population.[29]

Wylie's sentiments are shared by others, including some U.S. legislators. Appended to the SSCI report on Russian interference with the 2016 election were the additional views expressed by individual Senators, including Sen. Ron Wyden of Oregon, who noted that at one of the Committee's hearings:

> I asked Facebook's Chief Operating Officer Sheryl Sandberg and Twitter's Chief Executive Officer Jack Dorsey whether increased protections and controls to defend personal privacy should be a national security priority. Both witnesses answered in the affirmative. *Weak data privacy policies increase the ability of foreign adversaries to micro-target Americans for purposes of election interference.* Facebook's total failure to prevent Cambridge Analytica and Aleksandr Kogan from obtaining sensitive personal data about Facebook users, as well as Facebook's troubling data-sharing partnerships with Chinese smart phone manufacturers, demonstrate *clear gaps in federal data privacy laws and highlight obvious weaknesses that could be exploited in future influence campaigns*.[30]

The known and suspected connections between CA's work and the Russian government efforts are complicated.[31] However, it is clear that the same techniques that CA was using to influence the 2016 election were also top of mind for the internet trolls at the

28. *Id.* at 5–6.
29. *Id.* at 6.
30. 2 S. REP. NO. 116-290, at 84 (2020) (emphasis added).
31. *See generally* Testimony of Christopher Wylie, *supra* note 27, at 8–10.

Russian-government-backed Internet Research Agency (IRA). Details of those activities are described in the criminal indictment that resulted from the investigation led by Special Counsel Robert Mueller.[32] Since 2016, adversarial foreign governments have continued to use social media as a vector for influencing popular opinion and attempting to influence politics and election outcomes in the United States. During the 2020 presidential campaign season, social media platforms removed accounts linked to Cuba, Russia, Saudi Arabia, Thailand, and Iran.[33] Nor is the threat limited to the U.S., as Facebook has announced the removal of networks of inauthentic accounts sponsored by the governments of Russia and Iran that were spreading misinformation, it noted that those networks sought to disrupt elections in North Africa and Latin America as well as in the U.S.[34] Of course, social media can also be a powerful medium for the growth of democracy, as witnessed by the groundswell of popular support that led to the Arab Spring.[35] While the openness of social media can be a boon for speech and democracy, examples like the 2016 Russian active measures campaign demonstrate that it can also be leveraged to destabilize democracies. The use of detailed personal profiles as a way to target social media messaging relating to political, social, and cultural issues will likely continue to be a tactic that governments around the world exploit to influence public sentiment in years to come.

Second, cybersecurity. The SolarWinds hack announced in December 2020 was the latest in a series of high-profile cybersecurity attacks that are largely believed to have been carried out by the intelligence services of an adversarial foreign government.[36] The

32. *See* Criminal Indictment, United States v. Internet Rsch. Agency LLC, No. 1:18-cr-00032-DLF, 2018 WL 914777 (D.D.C. Feb. 16, 2018).

33. *See, e.g.*, Meysam Alizadeh et al., *Are Influence Campaigns Trolling Your Social Media Feeds?*, WASH. POST (Oct. 13, 2020, 6:00 AM), https://www.washingtonpost.com/politics/2020/10/13/are-influence-campaigns-trolling-your-social-media-feeds/; Julian E. Barnes & David E. Sanger, *Iran and Russia Seek to Influence Election in Final Days, U.S. Officials Warn*, N.Y. TIMES (Oct. 21, 2020), https://www.nytimes.com/2020/10/21/us/politics/iran-russia-election-interference.html.

34. *See* Eric Tucker, *Threat to US Elections in 2020 Is Not Limited to Russia*, AP NEWS (Oct. 30, 2019), https://apnews.com/article/1af297b4625c4dd585274dfaf1c39aeb.

35. Catherine O'Donnell, *New Study Quantifies Use of Social Media in Arab Spring*, UW NEWS (Sept. 12, 2011), https://www.washington.edu/news/2011/09/12/new-study-quantifies-use-of-social-media-in-arab-spring/ ("After analyzing more than 3 million tweets, gigabytes of YouTube content and thousands of blog posts, a new study finds that social media played a central role in shaping political debates in the Arab Spring. Conversations about revolution often preceded major events, and social media has carried inspiring stories of protest across international borders.")

36. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., COMMODIFICATION OF CYBER CAPABILITIES: A GRAND CYBER ARMS BAZAAR 4 (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

SolarWinds incident, also referred to by the moniker Sunburst, is named for the Texas-based technology company whose Orion software product suite was compromised by this incident.[37] Through a series of actions that cybersecurity researchers have assessed as being notably sophisticated and complex, cyber actors were able to inject malicious code into automated software updates that Orion users uploaded between March and June 2020, and then carry out further computer network operations on selected victims. The end result: as many as 18,000 SolarWinds customers may have uploaded the malicious code, enabling the hackers to launch additional exploits that gave them wide-ranging access to accounts, credentials, networks, and information of the exploited targets.

Although investigations into this incident were still ongoing at the time this article was being written, it has been widely—if informally—attributed to a group often referred to as APT29 or Cozy Bear, reliably believed to be the SVR component of the Russian government's intelligence services. The impact has been global, affecting government and private sector networks in the U.S., the United Kingdom, Canada, Mexico, Spain, Belgium, and elsewhere around the world. Within the U.S., the incident has been confirmed to have resulted in compromise of networks and accounts used by the Department of Justice, Department of Homeland Security, Department of Energy, Department of Commerce, and other government agencies.[38]

Although it is too soon to know precisely how personal information obtained through the SolarWinds incident may be used, other recent cyberattacks provide examples of the risks to personal data. The Equifax data breach resulted in the compromise of information relating to some 140 million Americans.[39] In January 2020,

37. SolarWinds provides a range of information technology security tools, including network monitoring products used by U.S. government agencies and companies around the world (including some 425 of the Fortune 500). *See* Jason Murdock, *Hacked Software Firm SolarWinds' Clients Include Ford, Microsoft, AT&T*, (Dec. 14, 2020, 6:08 AM), https://www.newsweek.com/solarwinds-hack-customer-list-suspected-russian-cyberattack-1554467#:~:text=SolarWinds%20says%20it%20serves%20more,branches%20of%20the%20U.S.%20military; *see also IT Security Management Tools*, SOLARWINDS, https://www.solarwinds.com/it-security-management-tools (last visited Feb. 14, 2021).

38. *See, e.g.*, Lucian Constantin, *SolarWinds Attack Explained: And Why It Was So Hard to Detect*, CSO (Dec. 15, 2020, 3:44 AM), https://www.csoonline.com/article/3601508/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html; David E. Sanger et al., *As Understanding of Russian Hacking Grows, So Does Alarm*, https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html (Jan. 5, 2021).

39. *See, e.g.*, Josh Fruhlinger, *Equifax Data Breach FAQ: What Happened, Who Was Affected, What Was the Impact?*, CSO (Feb. 12, 2020, 8:09 AM), https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html; U.S. GOV'T ACCOUNTABILITY OFF., GAO-18-559, DATA PROTECTION: ACTIONS TAKEN

the Department of Justice indicted four members of the Chinese military charged with carrying out the attack[40]—suggesting the hack was one of a number of cyber incidents believed to have been carried out by the People's Liberation Army and Chinese intelligence agencies.[41] Similarly, the cyberattack on the U.S. Office of Personnel Management, carried out in 2013–2014, resulted in the compromise of personal information of some 5 million government employees and contractors, as well as their family members and contacts—including the exceptionally detailed information contained in the SF-86 forms filled out by individuals applying for security clearances.[42] Like the Equifax incident, the OPM breach is widely believed to have been carried out by the Chinese government and is assessed to have provided a wealth of information that could be used for counterintelligence operations by the Chinese military and intelligence services.[43]

Wide-reaching cyber incidents like the supply chain attack on SolarWinds software and the data breaches involving Equifax and OPM threaten the integrity of critical infrastructure, personal information, commerce, and other national interests. Despite these risks, software companies are largely unregulated, with effective security measures being relegated to business decisions and perceived competitive advantage rather than requirements; and state data breach laws focus on providing notification to affected individuals, but few of these laws impose specific requirements that companies or other entities that collect or process personal information adopt specific cybersecurity measures.[44] While U.S. government

---

BY EQUIFAX AND FEDERAL AGENCIES IN RESPONSE TO THE 2017 BREACH 1 (2018) (available at https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf).

40. *See* Criminal Indictment, United States v. Zhiyong, No. 2:20-CD046 (N.D. Ga. Jan. 28, 2020).

41. *See, e.g.*, Katie Benner, *U.S. Charges Chinese Military Officers in 2017 Equifax Hacking*, N.Y. TIMES, https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html (May 7, 2020).

42. *See, e.g.*, MAJORITY STAFF REP. OF H.R. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED NATIONAL SECURITY FOR MORE THAN A GENERATION v–vi (Comm. Print 2016); Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO (Feb. 12, 2020, 8:15 AM), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

43. Ian Smith, *Bolton Confirms China Was Behind OPM Data Breaches*, FEDSMITH (Sept. 21, 2018, 5:00 PM), https://www.fedsmith.com/2018/09/21/bolton-confirms-china-behind-opm-data-breaches/.

44. One notable exception to this trend is the New York Department of Financial Services (NYDFS) Reg. 500, which requires entities that are licensed and regulated by the NYDFS to consider and adopt specific cybersecurity measures. N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2017).

departments and agencies with cybersecurity responsibilities can carry out foreign intelligence gathering and law enforcement investigation to identify emerging cyber risks, they—appropriately—lack authority to monitor private sector networks in the U.S. Thus, nation-state adversaries who attack private entities for geopolitical reasons find that those private networks, and the personal information they contain, are defended by private sector means—which can vary greatly in their level of cybersecurity preparedness and protection. Existing consumer protection measures, like state data breach notification laws, do little to address the underlying threat, or to provide meaningful assistance either to those private sector networks that are targeted or to the individuals whose personal data may be breached as a result.

Third, foreign counterintelligence operations. The Russian government's interference with the 2016 U.S. presidential election has included well-documented intelligence components alongside the social media campaigns.[45] Russia is not, however, the only adversarial foreign government about which the U.S. has had counterintelligence concerns. For example, in August 2020, William Evanina, then the Director of the National Counterintelligence and Security Center (NCSC) issued a statement warning that:

> [a]head of the 2020 U.S. elections, foreign states will continue to use covert and overt influence measures in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic process. . . . We are primarily concerned about the ongoing and potential activity by China, Russia, and Iran.[46]

The counterintelligence threat to the U.S. is, in the view of U.S. government officials and agencies, not limited to election security and integrity and democratic processes. In an address given in July 2020, Federal Bureau of Investigation (FBI) Director Christopher Wray cautioned that, "[t]he greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by

45. These efforts were documented at length by the Senate Select Committee on Intelligence. *See* 5 S. REP. NO. 116-290, at v (2020).

46. Press Release, William Evanina, Director, National Counterintelligence & Security Center, Election Threat Update for the American Public (Aug. 7, 2020, 1:07 PM), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

extension, to our national security."[47] Wray went on to articulate this threat at length over the course of his remarks, beginning with the most direct and personal impact on individuals. "If you are an American adult, it is more likely than not that China has stolen your personal data."[48] Noting the widespread impact of the Equifax hack, Wray continued, "[o]ur data isn't the only thing at stake here—so are our health, our livelihoods, and our security."[49] To underscore the magnitude of the threat, Wray noted that the FBI opened a new China-related counterintelligence investigation about every ten hours, and that China-related matters comprise nearly half of all counterintelligence investigations being actively worked by the FBI.[50] Specific areas of concern: "at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research[,]"[51] as well as being culpable for the OPM hack and the massive data breach that affected American health insurer Anthem, as well as the Equifax breach.[52] The potential harms were multi-faceted, according to Wray: compromise of the data itself; use of the data to feed and train the artificial intelligence algorithms being developed by the Chinese government; and using the information to identify Americans who can be targeted for human intelligence operations aimed at obtaining sensitive government information, to be recruited for covert malign influence operations, and to target Chinese nationals outside of China who are seen as threats to the current Chinese Communist Party (CCP) regime.[53] Director Wray described the longstanding concerns regarding Chinese government theft of U.S. intellectual property and noted the ways in which companies like Huawei, which makes networking equipment, could provide a vantage point for wide-ranging collection of information from individuals as well as across all sectors of the economy.[54]

Against this backdrop of concerns, 2019–2020 saw unprecedented focus by the U.S. government on Chinese-owned technology companies that had access to U.S. telecommunications infrastructure and

47. Christopher Wray, FBI Director, Address to the Hudson Institute: The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States (July 7, 2020).
48. *Id.*
49. *Id.*
50. *Id.*
51. *Id.*
52. *Id.*
53. *Id.*
54. *Id.*

personal information.[55] The Trump administration imposed additional tariffs on Chinese trade,[56] imposed sanctions on specific Chinese companies tied to the Chinese government and CCP,[57] and announced a ban—a mix of trade sanctions and consumer restrictions—on two popular mobile phone apps, TikTok and WeChat.[58] U.S. government entities had been eyeing TikTok warily as it grew in popularity, concerned about personal data being siphoned off by the Chinese government and with TikTok algorithms that seemed to suppress some content and promote other content in ways designed to please CCP censors. The company had already been fined by the FTC for violating children's privacy protection laws, investigated by the Committee on Foreign Investments in the U.S. (CFIUS), and banned by the U.S. Navy—all the while, however, the app continued to gain subscribers in the U.S.[59] Against this backdrop, in August 2020, then-President Trump signed an EO banning various commercial transactions with TikTok.[60] The EO made broad allegations that "the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States."[61] However, although commentators have pointed out that there are genuine risks that users' personal information might be harvested by the Chinese government in ways that undermine personal privacy and free speech and create counterintelligence risks,[62] they have also

55. The U.S. government measures included actions against Huawei and Executive Order 13,959, announcing new sanctions against Chinese-owned companies, signed by then-President Donald Trump on November 12, 2020. Those actions, although relevant for context, are not addressed in any detail in this article. *See* Exec. Order No. 13959, 85 Fed. Reg. 73,185 (Nov. 12, 2020); *see also* Sherisse Pham, *New US Sanctions Could Slowly Strangle Huawei's Smartphone Business*, CNN BUS., https://edition.cnn.com/2020/08/14/tech/huawei-kirin-chipsets-hnk-intl/index.html (Aug. 14, 2020, 12:02 AM).

56. Tom Lee & Jacqueline Varas, *The Total Cost of U.S. Tariffs*, AM. ACTION F. (Sept. 16, 2020), https://www.americanactionforum.org/research/the-total-cost-of-trumps-new-tariffs/.

57. Humeyra Pamuk & Matt Spetalnick, *U.S. Preparing New Sanctions on Chinese Officials over Hong Kong Crackdown*, REUTERS (Dec. 6, 2020, 8:19 PM), https://www.reuters.com/article/usa-china-sanctions/exclusive-u-s-preparing-new-sanctions-on-chinese-officials-over-hong-kong-crackdown-sources-idUSL4N2IN0AO; *see* Exec. Order No. 13,959, 85 Fed. Reg. 73,185 (Nov. 12, 2020).

58. Tali Arbel et al., *US Bans WeChat, TikTok from App Stores, Threatens Shutdowns*, AP NEWS (Sept. 18, 2020), https://apnews.com/article/national-security-china-archive-united-states-a439ead01b75fc958c722daf40f9307c.

59. *See, e.g.*, Rita Liao & Catherine Shu, *TikTok's Epic Rise and Stumble*, TECHCRUNCH (Nov. 26, 2020, 4:11 AM), https://techcrunch.com/2020/11/26/tiktok-timeline/.

60. Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020); *see also* Press Release, U.S. Dep't of Com., *supra* note 58.

61. Exec. Order No. 13,942, 85 Fed Reg. 48,637.

62. *See, e.g.*, Lindsay Gorman, *Q&A with Lindsay Gorman: How Does TikTok Pose a National Security Risk to the United States?*, GERMAN MARSHALL FUND (Aug. 25, 2020),

noted that the EO did little to make clear the precise nature of the concerns and how this EO might meaningfully address them.[63] According to one critic, the ban was inarticulate and vague: "[d]epending on one's perspective, concerns might be raised about TikTok collecting data on U.S. government employees, TikTok collecting data on U.S. persons not employed by the government, . . . TikTok censoring information *beyond* China at Beijing's behest, or disinformation on the TikTok platform."[64] For other commentators, the ban risked sending the U.S. down the road to totalitarianism, as:

> "the blunt, chaotic and process-free unilateral action on TikTok has failed to draw a clear distinction between democratic and autocratic measures taken in the name of national security. In the absence of clearly defined criteria around ownership, data storage, data access and algorithmic influence—all thorny components of the global information contest in which democracies find themselves—the United States risks emulating the authoritarian model" for dealing with technology platforms and providers.[65]

Meanwhile, as TikTok litigated the validity of the EO, the risks of authoritarian misuse of personal data were underscored in a lawsuit filed by WeChat users against the app's parent company, Tencent, alleging that user accounts were cut off precisely because of Chinese government surveillance and censorship of app users' chats.[66]

Shortly after inauguration, (when this article was being prepared for publication), the Biden-Harris administration had reportedly not yet made a decision about whether to continue to or change course on the previous administration's position on TikTok and

---

https://securingdemocracy.gmfus.org/qa-with-lindsay-gorman-how-does-tiktok-pose-a-national-security-risk-to-the-united-states/.

63. *See, e.g.*, Justin Sherman, *Building a Better U.S. Approach to TikTok and Beyond*, LAWFARE (Dec. 28, 2020, 10:25 AM), https://www.lawfareblog.com/improving-tech-policy ("The Trump administration's TikTok executive order was more of a tactical move against a single tech firm than a fully developed policy. . . . Going forward, any executive branch policy on foreign software needs to explicitly specify the scope of the cybersecurity concerns at issue," which might include targeted foreign espionage through software systems, censorship conducted by foreign-owned platforms, and foreign governments "potentially collecting massive amounts of U.S. citizen data through software.").

64. *Id.*

65. Lindsay Gorman, *A Way Forward for U.S. Policy on TikTok*, LAWFARE (Nov. 10, 2020, 8:01 AM), https://www.lawfareblog.com/way-forward-us-policy-tiktok.

66. *See, e.g.*, Bloomberg, *Six California WeChat Users Sue Tencent for Alleged Chat Surveillance*, L.A. TIMES (Jan. 11, 2021, 6:22 PM), https://www.latimes.com/business/story/2021-01-11/california-wechat-users-sue-tencent-for-alleged-surveillance.

Huawei.[67] Whatever approach the new administration adopts, these issues of the vulnerability and collection of personal and corporate information by adversarial foreign governments is sure to remain a concern—as are the ways in which personal information and tech platforms are similarly used to influence domestic terrorism, civil discourse, and even insurrection.

Fourth, domestic terrorism and insurrection. On October 8, 2020, federal officials unsealed charges against thirteen people who had, according to the indictment, plotted to kidnap Michigan Governor Gretchen Whitmer, attack law enforcement, overthrow the government, and start a civil war.[68] The plot was shocking in its details: the suspects, part of a self-styled militia group in Michigan, had participated in field training exercises, created improvised explosive devices, and developed a detailed plan to kidnap Whitmer from her personal vacation home or official summer residence. They bought specialized equipment for a nighttime raid, took photographs and video of the vacation home, and made plans to blow up a nearby bridge to impede the ability of police to respond. At least some of the plotters appeared, from their comments, to be prepared to kill Governor Whitmer.[69]

Social media played a key role in the criminal conspiracy: according to the indictment, the men carried out much of their planning on and through private groups on Facebook. Experts in disinformation were quoted at the time as saying, "[s]ocial media companies have been allowing these communities to build and grow, ignoring the mounting evidence that memes, posts and images encouraging violence can and do translate into actual violence[.]"[70] Perhaps this should have been no surprise, as researchers had been warning for some time about the spread of far-right extremism on the internet. Following the August 2017 Unite the Right rally in Charlottesville, Virginia, social scientists pointed to the ways in which social media was serving as a recruiting ground for white supremacist groups.[71]

67. *See, e.g.*, Sean Lyngaas, *No Decisions Yet on Any Changes to TikTok or Huawei Cases, White House Says*, CYBERSCOOP (Jan. 25, 2021), https://www.cyberscoop.com/huawei-tiktok-china-biden-white-house/.

68. *See* Affidavit of FBI Special Agent Richard J. Trask II, United States v. Fox, No. 1:20-mj-00416-SJB (W.D. Mich. Oct. 16, 2020), ECF No. 1-1.

69. *Id.* at 7–8 ("Have one person go to her house. Knock on the door and when she answers it just cap her . . . catch her walking into the building and act like a passers-by and fixing dome her then yourself . . . ."); *id.* at 13 ("Kidnapping, arson, death. I don't care.").

70. Craig Timberg & Isaac Stanley-Becker, *Michigan Kidnapping Plot, Like So Many Other Extremist Crimes, Foreshadowed on Social Media*, WASH. POST (Oct. 8, 2020, 6:42 PM), https://www.washingtonpost.com/technology/2020/10/08/michigan-plot-kidnapping-boogaloo-socialmedia/ (quoting Cindy Otis, Vice President of Analysis for Aletha Group).

71. Francie Diep, *How Social Media Helped Organize and Radicalize America's White Supremacists*, PAC. STANDARD (Aug. 15, 2017), https://psmag.com/social-justice/how-social-

The protest had been a deadly and brazen display of white supremacist ideology in which a woman was killed when a man drove his car into a crowd of peaceful counter-demonstrators.[72] The man who drove the car was only twenty years old, but reportedly deeply immersed in white supremacist ideology.[73]

Research remains ongoing to better understand what makes individuals susceptible to radicalization, and how to counteract those forces. There is consensus, however, that the internet, and social media in particular, play a role. According to one expert, the key components for radicalization are an individual's quest for significance, encountering a narrative that serves as a vehicle for that significance, and having a network of support for those views.[74] Although we do not know how much impact social media and online radicalization may have had on this man's decision to drive his car into a crowd of protestors, we know that the Unite the Right rally was planned on Facebook.[75] And we know that Facebook's own research has shown that nearly two-thirds of the platform's users to join extremist groups on Facebook do so after Facebook's own algorithms recommend the extremist groups to them.[76]

The issues have become more urgent since 2017, as a toxic mix of disinformation has spread online, ranging from the QAnon conspiracy theory to baseless allegations of election fraud, and from white supremacist ideology to fact-free claims that the coronavirus is a hoax and that COVID vaccines will be used to inject people with microchips.[77]

None of these conspiracy theories or ideologies exists solely online; to greater and lesser extents, they spread offline as well. But in order to achieve maximum scope and reach, all of these threat vectors depend on access to the massive quantities of

---

media-helped-organize-and-radicalize-americas-newest-white-supremacists ("[T]he tools of the Internet Age have helped white supremacists and other bigots to share ideas and organize.").

72. Mitch Smith, *James Fields Sentenced to Life in Prison for Death of Heather Heyer in Charlottesville*, N.Y. TIMES (June 28, 2019), https://www.nytimes.com/2019/06/28/us/james-fields-sentencing.html.

73. Alexa Liautaud, *How the Charlottesville Suspect Became Radicalized*, VICE NEWS (Aug. 14, 2017, 3:14 PM), https://www.vice.com/en/article/zmy8n8/how-the-charlottesville-attacker-became-radicalized.

74. *Id.*

75. Diep, *supra* note 71.

76. Jeff Horwitz & Deepa Seetharaman, *Facebook Executives Shut Down Efforts to Make the Site Less Divisive*, WALL ST. J. (May 26, 2020, 11:38 AM), https://www.wsj.com/articles/facebook-knows-it-encourages-division-top-executives-nixed-solutions-11590507499.

77. *See, e.g.*, Jack Goodman & Flora Carmichael, *Coronavirus: Bill Gates 'Microchip' Conspiracy Theory and Other Vaccine Claims Fact-Checked*, BBC (May 30, 2020), https://www.bbc.com/news/52847648.

personal information and the detailed personal behavioral profiles that make targeted advertising, recommender algorithms, private groups, and other key tools of information—and disinformation—spread and targeted messaging possible in today's digital ecosystem.

The cumulative frenzy of this partially-online ecosystem spilled over into real life on January 6, 2021, when a mob of right-wing protesters stormed the U.S. Capitol building in an attempt to prevent certification of the Electoral College votes that would formalize Joe Biden's win in the 2020 U.S. presidential election.[78] Even as events were unfolding, experts quickly pointed to the fact that the attempted insurrection had been hiding in plain sight for weeks or months, organized on social media.[79]

In some respects, this should have come as no surprise. Online radicalization had been a source of concern in the national security community for decades. In the aftermath of the terrorist attacks of 9/11, the U.S. government and intelligence agencies around the world were pouring time and energy into understanding how the internet had become a vehicle for radicalizing supporters of al-Qaeda and other international terrorist groups.[80] By 2011, analysts in the U.S. who were studying online radicalization were still often focused on older internet technologies such as web forums, closed communities of anonymous users where groups like al-Qaeda proselytized to its members and newer recruits found inspiration.[81] There was some recognition, however, of the power of the internet and the ways in which the technology was impacting radicalization:

> [c]omputers affect how we experience media and how we interact with others. Extremists are as susceptible to these effects

78. Dan Barry et al., *'Our President Wants Us Here': The Mob That Stormed the Capitol*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/us/capitol-rioters.html (Feb. 13, 2021); Amy Brittain et al., *The Capitol Mob: A Raging Collection of Grievances and Disillusionment*, WASH. POST (Jan. 10, 2021), https://www.washingtonpost.com/investigations/2021/01/10/capitol-rioters-identified-arrested/?arc404=true; *Mob Attack, Incited by Trump, Delays Election Certification*, N.Y. TIMES, https://www.nytimes.com/live/2021/01/06/us/electoral-vote (Jan. 20, 2021, 11:40 AM).

79. *See, e.g.*, Sheera Frenkel, *The Storming of Capitol Hill Was Organized on Social Media*, N.Y. TIMES (Jan. 6, 2021, 4:41 PM), https://nyti.ms/3q0L6dn.

80. *See, e.g.*, Dana Janbek & Valerie Williams, *The Role of the Internet Post-9/11 in Terrorism and Counterterrorism*, 20 BROWN J. WORLD AFFS. 297 (2014); *see also Jihadist Use of Social Media—How to Prevent Terrorism and Preserve Innovation*: *Hearing Before the Subcomm. on Counterterrorism & Intel. of the Comm. on Homeland Sec.*, 112th Cong. 14 (2011) (testimony of Andrew Aaron Weisburd) ("The U.S. intelligence community is already making very effective use of the internet to identify and investigate extremists.") [hereinafter *Jihadist Use of Social Media*].

81. *See, e.g.*, *Jihadist Use of Social Media*, *supra* note 80, at 11 (testimony of Andrew Aaron Weisburd).

> as we are. The on-line environment is immersive. We feel we are in a place, often called cyberspace. When we are on a social media site, we feel that we are virtually together with our friends, family, and comrades in arms. We feel we are present in the videos we watch. On-line interaction brings people closer, faster. On-line relationships get off to a strong start, and then move off-line if possible.[82]

However, as evidenced by one expert's comments, there still was an understanding that social networks largely mirrored offline networks—and perhaps underestimated the extent to which social media would be shaping offline networks and driving offline behavior, either then or in the future.[83] Perhaps for this reason, much of the focus was on countering slickly produced films, digital magazines, and other media produced by terrorist organizations, rather than anticipating the ways in which the interactive nature of the internet itself would make radical recruitment messaging harder to resist.

Branding in terrorist media is a sign of authenticity, and terrorist media is readily identifiable as such due to the presence of trademarks known to be associated with particular organizations. The objective should be not to drive all terrorist media off-line, but to drive it to the margins and deprive it of the power of branding, as well as to leave homegrown extremists unable to verify the authenticity of any given product.[84]

The witnesses were not interested in deplatforming terrorists—on the contrary, they pointed out that law enforcement benefited greatly from the ability to track the connections and communications between and among suspected terrorist actors online.[85]

---

82. *Id.* at 13.

83. *Id.* ("On-line social networks tend to mirror off-line social networks. People—extremists included—use social media to keep in touch with people they already know. An individual's ability to get involved in terrorism is directly related to who they know, and this is precisely what social media sites reveal to us.").

84. *Id.* at 14.

85. *See id.* at 13 ("An individual's ability to get involved in terrorism is directly related to who they know, and this is precisely what social media sites reveal to us. The benefits of this to law enforcement are enormous.") (testimony of Andrew Aaron Weisburd). The Senior Advisor to the President, Rand Corporation continued:

> this on-line discussion and these postings are a source of valuable intelligence. So rather than devoting vast resources to shutting down content and being dragged into a frustrating game of whack-a-mole—as we shut down sites, they open up new ones. Instead, we probably should devote our resources to facilitating intelligence collection and criminal investigations so that we can continue to achieve the successes that we have had thus far in identifying these individuals, uncovering these plots and apprehending these individuals.

Id. at 15 (testimony of Brian Michael Jenkins).

Just five years later, the government's approach to countering violent extremism had expanded to recognize the growing role of social media interactions in addition to display of propagandistic content.[86] In the wake of the Orlando nightclub shooting, a senior official at the Department of Homeland Security explained:

> [t]he threat from homegrown violent extremism requires going beyond traditional counterterrorism approaches and focusing not just on mitigation efforts but also on preventing and intervening in the process of radicalization. This prevention framework is known as "countering violent extremism," or the acronym CVE. . . . Terrorist groups such as ISIL have undertaken a deliberate strategy of using social media to reach individuals susceptible to their message and recruit and inspire them to violence.[87]

Perhaps naïvely, in 2011 at least one expert noted that,

> [p]roducing and distributing media for Foreign Terrorist Organizations constitutes material support for terrorism. I would argue that a service provider who knowingly assists in the distribution of terrorist media is also culpable. While it is in no one's interests to prosecute internet service providers, they must be made to realize that they can neither turn a blind eye to the use of their services by terrorist organizations, nor can they continue to put the onus of identifying and removing terrorist media on private citizens. I don't believe that Google, operator of YouTube, has an interest in promoting violent

86. *See, e.g.*, *Isis Online: Countering Terrorist Radicalization and Recruitment on the Internet and Social Media: Hearing Before the Permanent Subcomm. on Investigations of the Comm. on Homeland Sec. and Governmental Affs.*, 114th Cong. (2016). Michael Steinbach, Executive Assistant Director, National Security Branch, FBI stated,

> ISIL's messaging blends both officially endorsed sophisticated propaganda with that of informal peer-to-peer recruitment through digital communication platforms. No matter the format, the message of radicalization spreads faster than we imagined just a few years ago. Like never before, social media allows for overseas terrorists to reach into our local communities to target our citizens as well as to radicalize and recruit.

Id. at 8; *see also id.* at 11–12 (testimony of Meagen M. LaGraffe, Chief of Staff to the Coordinator and Special Envoy, Global Engagement Center, U.S. Department of State) ("[W]hile al-Qaeda was producing videos that took months to get out, our adversary today is using social media in ways not seen before.").

87. *Id.* at 10 (testimony of George Selim, Director, Office of Community Partnerships, U.S. Department of Homeland Security, and Director, Interagency Task Force on Countering Violent Extremism).

> extremism, and they have already made some effort to address this issue, but they can and should do more.[88]

That expert might have been surprised to see the politically charged debates taking place a decade later over content moderation and deplatforming of accounts both before and after the mob assault on the Capitol in 2021.

IV. PRIVACY AND NATIONAL SECURITY ARE NOT ALL: THE INTERSECTIONS AMONG DEPLATFORMING, CONTENT MODERATION, ANTITRUST, AND ONLINE HARMS

To put the growth of online conspiracy theories and disinformation into context, it is useful to remember the recency of social media as a communication tool, and of complex and detailed personal being collected as a ubiquitous part of daily life. Facebook was launched in 2004.[89] Since then, the platform and its family of apps has amassed nearly 3 billion users—nearly half the world's population.[90] The first smartphone became available when the iPhone entered the market in 2007,[91] and smartphones are now used by an estimated 3.8 billion people around the world.[92] Data brokers create personal profiles based on thousands of data points about individuals,[93] in a business worth an estimated $200 billion.[94] The online profiling carried out by data brokers and platforms is not limited to location, demographic facts, or behavior; it also includes personality modeling and behavioral prediction. Perhaps the most

---

88. *Jihadist Use of Social Media*, *supra* note 80, at 14 (testimony of Andrew Aaron Weisburd).

89. Mark Hall, *Facebook*, BRITANNICA, https://www.britannica.com/topic/Facebook (Feb. 4, 2021).

90. Facebook recorded some 2.6 billion active users in the third quarter of 2020, and its family of apps—Facebook, WhatsApp, Instagram—surpassed 3 billion users in the first quarter of 2020. *See* H. Tankovska, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2020*, STATISTA (Feb. 2, 2021), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/; *see also* Khari Johnson, *Facebook Apps Now Used Monthly by More than 3 Billion People*, VENTUREBEAT (Apr. 29, 2020, 2:31 PM), https://venturebeat.com/2020/04/29/facebook-earnings-q1-2020/.

91. John Markoff, *Apple Introduces Innovative Cellphone*, N.Y. TIMES (Jan. 10, 2007), https://www.nytimes.com/2007/01/10/technology/10apple.html.

92. S. O'Dea, *Number of Smartphone Users Worldwide from 2016 to 2023*, STATISTA (Mar. 18, 2021), https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

93. *See, e.g.*, Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators Try to Rein in the 'Privacy Deathstars'*, FIN. TIMES (Jan. 8, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521.

94. David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019, 8:00 AM), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

notorious recent example of this took place on Facebook, which has used information about users' behavior both on and off the platform to assess where individuals fell within the set of personality traits measured by the "OCEAN" standard of a person's tendency towards Openness, Conscientiousness, Extroversion, Agreeableness, and Neuroticism,[95] and to assess its users' behavior and personalities so thoroughly that, according to at least one study, Facebook's algorithms were more accurate at predicting an individual's personality traits than even their own family members.[96]

The Silicon Valley industry that was once heralded as the hub of global innovation has, in recent years, come under increasing scrutiny by privacy advocates, antitrust regulators, and legislators in the U.S. and Europe over concerns ranging from market dominance to intrusive data collection practices.[97] December 2020 brought illustrative examples, with three significant measures likely to impact the future of data-driven platforms and cross-platform data sharing.

In the first, the FTC filed a complaint against Facebook, charging the company with anticompetitive practices tied to its purchase of Instagram and WhatsApp and the policies through which Facebook restricts the activities of third party developers who create online services designed to connect to the Facebook platform.[98] The complaint, which focuses on monopolistic practices and market effects, refers to privacy impacts as well, noting that if there were greater competition in social media, benefits to users could include rival platforms that offer greater data protection options for users.[99]

Just a week later, the FTC announced that it was launching an inquiry into the privacy practices of the major social media and

95. *See, e.g.*, Erin Brodwin, *Here's the Personality Test Cambridge Analytica Had Facebook Users Take*, BUS. INSIDER (Mar. 19, 2018, 4:01 PM), https://www.businessinsider.com/facebook-personality-test-cambridge-analytica-data-trump-election-2018-3.

96. *See, e.g.*, Frank Luerweg, *The Internet Knows You Better than Your Spouse Does*, SCI. AM. (Mar. 14, 2019), https://www.scientificamerican.com/article/the-internet-knows-you-better-than-your-spouse-does/; Douglas Quenqua, *Facebook Knows You Better than Anyone Else*, N.Y. TIMES (Jan. 19, 2015), https://www.nytimes.com/2015/01/20/science/facebook-knows-you-better-than-anyone-else.html.

97. *See, e.g.*, Adam Satariano, *'This Is a New Phase': Europe Shifts Tactics to Limit Tech's Power*, N.Y. TIMES (July 30, 2020), https://www.nytimes.com/2020/07/30/technology/europe-new-phase-tech-amazon-apple-facebook-google.html; Daisuke Wakabayashi et al., *13 Ways the Government Went After Google, Facebook and Other Tech Giants This Year*, N.Y. TIMES, https://www.nytimes.com/interactive/2020/technology/tech-investigations.html (Dec. 16, 2020).

98. Press Release, Federal Trade Commission, FTC Sues Facebook for Illegal Monopolization (Dec. 9, 2020), https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization; Complaint at 1, FTC v. Facebook, Inc., No. 1:20-cv-03590-JEB (D.D.C. Jan. 13, 2021), ECF No. 51.

99. Complaint, *supra* note 98, at 12.

video streaming services, including Facebook, YouTube, ByteDance, Twitch, Reddit, and Discord.[100] The accompanying fifty-three-page Order catalogues an extensive list of information that the FTC is seeking, including user counts, usage statistics, and financial data, as well as questions that get to the heart of the platforms' business models, such as the nature of each user attribute that the platforms use, track, estimate, or derive about their users; the dollar value to the platforms of their users; and the nature of algorithms run on the platforms.[101]

At the same time, the UK announced that it was moving forward with a set of legislation intended to address online harms that included terrorist groups and gangs using online platforms for recruitment and radicalization of new members.[102] The proposals were first introduced in April 2019, and the December 2020 announcement signaled the end of the consultation period and implementation of the new approach[103] with issuance of interim codes of practice intended to address a number of online ills, including terrorist content and activity online.[104] The UK legislation carries with it echoes of the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Content Online[105] that followed the terrorist attack on two New Zealand mosques,[106] as well as laws in France and Germany and legislative proposals elsewhere that are directed at countering violent extremism and requiring minimum standards of content moderation for certain kinds of content posted

100. Press Release, Federal Trade Commission, Joint Statement of FTC Commissioners Chopra, Slaughter, and Wilson Regarding Social Media and Video Streaming Service Providers' Privacy Practices (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/public_statements/1584150/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

101. FTC Res. P205402 (2020).

102. The legislation is also aimed at curbing other forms of online harms, such as child sexual exploitation and abuse and drug trafficking. Press Release, Dep't for Digital, Culture, Media & Sport, UK to Introduce World First Online Safety Laws (Apr. 8, 2019), https://www.gov.uk/government/news/uk-to-introduce-world-first-online-safety-laws.

103. Caroline Dinenage, *Consultation Outcome: The Government Report on Transparency Reporting in Relation to Online Harms*, GOV.UK, https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/government-transparency-report (Dec. 15, 2020); Baroness Morgan of Cotes & Priti Patel, *Consultation Outcome: Online Harms White Paper—Initial Consultation Response*, GOV.UK, https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response (Dec. 15, 2020).

104. *Online Harms: Interim Codes of Practice*, GOV.UK (Dec. 15, 2020), https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice.

105. *ChristChurch Call: To Eliminate Terrorist and Violent Extremist Content Online*, CHRISTCHURCH CALL, https://www.christchurchcall.com/call.html (last vistited Feb. 14, 2020).

106. *Id.*

online.[107] Although the UK guidance on online harms is tied to definitions in the UK Terrorism Act of 2006, the kinds of activities it seeks to address include those that have been the focus of efforts to counter violent extremism worldwide, such as online statements that glorify, encourage, incite, or provide inducements for terrorist activities[108]—precisely the kinds of discourse that are central to the U.S. federal charges against Capitol rioters[109] and the House impeachment managers in considering how to present the impeachment case against former president Donald J. Trump for inciting an insurrection that erupted into violence on January 6, 2021.[110]

One of the most striking responses to online disinformation and the provocation of offline violence came from platform providers in the wake of the January 6 attack on the Capitol.[111] Within days, then-President Trump had been deplatformed—his account removed—from Twitter, Facebook, Twitch, and other major social media sites, and major Trump-oriented channels had been removed from other sites, such as Reddit's r/TheDonald and The Donald server on Discord.[112] Meanwhile, the far-right platform Parler was

---

107. *See Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act*, *NetzDG*), BUNDESMINISTERIUM DER JUSTIZ AND FÜR VERBRAUCHERSCHUTZ (2017), https://www.bmjv.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html; *see also* Loi 2020-766 du 24 Juin 2020 de Proposition de loi visant a lutter contre les contenus haineux sur internet [Law 2020-766 of June 24, 2020 on Fighting Hate on the Internet], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O. OFFICIAL GAZETTE OF FRANCE], June 25, 2020. The main provisions of the proposition were declared unconstitutional by the French Constitutional Council on June 18, 2020. *See French Avia Law Declared Unconstitutional: What Does This Teach Us at EU Level?*, EDRI (June 24, 2020), https://edri.org/our-work/french-avia-law-declared-unconstitutional-what-does-this-teach-us-at-eu-level/; *see also Current Approaches to Terrorist and Violent Extremist Content Among the Global Top 50 Online Content-Sharing Services*, ORG. FOR ECON. CO-OPERATION & DEV. 19–25 (Aug. 14, 2020), http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CDEP(2019)15/FINAL&docLanguage=En.

108. INTERIM CODE OF PRACTICE ON TERRORIST CONTENT AND ACTIVITY ONLINE 16–17 (2020), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944036/1704b_ICOP__online_terrorist_content_v.2_11-12-20.pdf.

109. Press Release, U.S. Dep't of Justice, Thirteen Charged in Federal Court Following Riot at the United States Capitol (Jan. 8, 2021), https://www.justice.gov/opa/pr/thirteen-charged-federal-court-following-riot-united-states-capitol; Marie Fazio, *Notable Arrests After the Riot at the Capitol*, N.Y. TIMES, https://www.nytimes.com/2021/01/10/us/politics/capitol-arrests.html (Mar. 5, 2021).

110. *See* Mike DeBonis et al., *House Democrats Building Elaborate, Emotionally Charged Case Against Trump*, WASH. POST (Jan. 29, 2021, 8:21 PM), https://www.washingtonpost.com/politics/house-democrats-building-elaborate-emotionally-charged-case-against-trump/2021/01/29/d35170fe-626c-11eb-9061-07abcc1f9229_story.html; Nicholas Fandos, *Trump Impeached for Inciting Insurrection*, N.Y. TIMES, https://www.nytimes.com/2021/01/13/us/politics/trump-impeached.html (Feb. 12, 2021).

111. Frenkel, *supra* note 79.

112. Sara Fischer & Ashley Gold, *All the Platforms That Have Banned or Restricted Trump So Far*, AXIOS, https://www.axios.com/platforms-social-media-ban-restrict-trump-d9e44f3c-8366-4ba9-a8a1-7f3114f920f1.html (Jan. 11, 2021).

removed from the Apple and Google app stores, and Amazon Web Service announced it would no longer host Parler, making the platform essentially unavailable for download (from app stores) or use (with no hosting platform).[113] These moves have prompted litigation,[114] and come at a time when politicians and activists across the political spectrum were already issuing widespread calls to reform Section 230 of the Communications Decency Act, the often-misunderstood provision of federal law that grants online platforms immunity from liability for content posted by their users.[115] Despite widespread complaints from the political right that its views were being silenced on social media, the data prior to January 6, 2021 demonstrated otherwise, with research from Facebook-owned CrowdTangle consistently showing that the top-performing posts on Facebook came from conservative commentators and outlets.[116]

Post-January 6, the landscape is less clear, as it may take some time for additional data to emerge. However, extremist alt-right content is likely to continue to be readily available in the U.S. The conclusion reached by some: "[I]t's likely that fringe and extremist websites will continue to seek refuge in other jurisdictions like Russia and China where they can more readily withstand diplomatic, political, and legal pressure."[117] This analysis underscores the intersection between national security, geopolitics, domestic extremism, and online outlets. Or, put more succinctly, "[t]he founder of neo-Nazi rag the *Daily Stormer* had some advice for the people who

---

113. *See, e.g.*, Jack Nicas & Davey Alba, *Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters*, N.Y. TIMES, https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html (Jan. 13, 2021); Sarah Perez, *This Week in Apps: Parler Deplatformed, Alt Apps Rise, Looking Back at 2020 Trends*, TECHCRUNCH (Jan. 16, 2021, 11:00 AM), https://techcrunch.com/2021/01/16/this-week-in-apps-parler-deplatformed-alt-apps-rise-looking-back-at-2020-trends/.

114. *See, e.g.*, Bobby Allyn, *Judge Refuses to Reinstate Parler After Amazon Shut It Down*, NPR (Jan. 21, 2021, 3:14 PM) https://www.npr.org/2021/01/21/956486352/judge-refuses-to-reinstate-parler-after-amazon-shut-it-down.

115. *See, e.g.*, David McCabe, *Tech Companies Shift Their Posture on a Legal Shield, Wary of Being Left Behind*, N.Y. TIMES (Dec. 15, 2020), https://www.nytimes.com/2020/12/15/technology/tech-section-230-congress.html; Daisuke Wakabayashi, *Legal Shield for Social Media Is Targeted by Lawmakers*, N.Y. TIMES, https://www.nytimes.com/2020/05/28/business/section-230-internet-speech.html (Dec. 15, 2020).

116. *See, e.g.*, Oliver Darcy, *Trump Says Right-wing Voices Are Being Censored. The Data Says Something Else*, CNN BUS., https://www.cnn.com/2020/05/28/media/trump-social-media-conservative-censorship/index.html (May 28, 2020, 7:54 PM); Mark Scott, *Despite Cries of Censorship, Conservatives Dominate Social Media*, POLITICO, https://www.politico.com/news/2020/10/26/censorship-conservatives-social-media-432643 (Oct. 27, 2020, 1:38 PM).

117. Fergus Ryan, *Why Are Moscow and Beijing Happy to Host the U.S. Far-Right Online?*, FOREIGN POL'Y (Jan. 22, 2021, 1:37 PM), https://foreignpolicy.com/2021/01/22/russia-beijing-web-host-far-right-parler-daily-stormer/.

ran Parler, after the app was purged from the Internet last week: Ask China or Russia for help."[118]

In the words of the United Kingdom's Digital Secretary Jeremy Wright, "[t]he era of self-regulation for online companies is over."[119]

V. LESSONS IN OVERSIGHT—AND HOW TO IMPROVE PRIVACY AND DATA PROTECTIONS WHILE ALLOWING REASONABLE GOVERNMENT USE

There are a number of sound reasons why legal theories relating to the regulation of government access to data is more mature, with jurisprudence of longer standing, than legal theories addressing private sector use of data—but the two areas of law may have useful lessons for each other. The scope of government power and the consequences of its misuse, America's historical roots in rebellion against a tyrannical regime, and the language of the Constitution itself, along with historical examples of government misuse of personal data, are among the reasons for focusing on harms, remedies, and constraints involving government use of information. For example, government misuse of personal information during the decades from World War II through the Vietnam War have been investigated and extensively documented, including in the Congressional hearings in the specially-designated Committees for intelligence oversight that came to be colloquially known as the Church and Pike Committees. The multi-volume report issued by the Senate's Church Committee incorporated a wealth of details about government overreach, as well as recommendations for how to prevent similar abuses going forward.[120] During the course of the Church and Pike Committee hearings, it became evident that there were multiple reasons for the challenges that Congress faced in overseeing the U.S. intelligence community documented by the Church and Pike Committees, including gaps in committee jurisdiction and insufficient resources and expertise to grapple with the implications of emerging technology.[121] The outcome was recognition of the need

118. *Id.*

119. UK to Introduce World First Online Safety Laws, *supra* note 102 (quoting the comments of Jeremy Wright accompanying the release of *Online Harms White Paper*).

120. Although the House of Representatives' Pike Committee never issued a final report, the transcripts of its hearings remain available, and excerpts from a draft version of the report were published in the newspaper *The Village Voice*. *See generally The CIA Report the President Doesn't Want You to Read*, VILL. VOICE (Feb. 16, 1976), https://www.villagevoice.com/1976/02/16/the-cia-report-the-president-doesnt-want-you-to-read/.

121. *See* April Falcon Doss, *Time for a New Tech-Centric Church-Pike: Historical Lessons from Intelligence Oversight Could Help Congress Tackle Today's Data-Driven Technologies*, 15 J. BUS. & TECH. L. 1, 1–2 (2019).

for a multifaceted approach that included all three branches of government, resulting in Executive Orders, legislation, judicial involvement in reviewing electronic surveillance, and the establishment of standing Congressional oversight committees. The work of those committees created a sweeping set of boundaries on the USIC, along with a comprehensive framework for oversight that has endured and, by and large, served the nation's multiple interests—protection of national security and of civil liberties and privacy—well.

Even within this framework, there have been a number of government programs that have raised legal or Constitutional questions or objections. For example, the NSA's bulk metadata collection program, first revealed through unauthorized disclosures by former government contractor Edward Snowden,[122] quickly prompted concerns over the program's legality, with groups like the American Civil Liberties Union (ACLU) arguing that the program violated the PATRIOT Act as well the First and Fourth Amendments to the Constitution.[123] The program had, in fact, been reviewed and approved dozens of times by independent judges sitting on the Foreign Intelligence Surveillance Court (FISC),[124] and the program had been briefed to members of Congress.[125] But the program had never previously been publicly disclosed, and there was little about the statutory language or the legal premises upon which the program relied that would have given the public at large reason to think that such activities were happening.[126] In other words, for

122. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 PM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

123. *See, e.g.*, Press Release, ACLU, ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program (June 11, 2013), https://www.aclu.org/press-releases/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program?redirect=national-security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program.

124. *See, e.g.*, Scott F. Mann, *Fact Sheet: Section 215 of the USA PATRIOT Act*, CSIS (Feb. 27, 2014), https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act; *see also Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing Before the S. Comm. on the Judiciary*, 113 Cong. 113–334 (2013) (statement of James M. Cole, Deputy Attorney General of the U.S.); *see also In re* Application of the Fed. Bureau of Investigation for an Ord. Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

125. *In re Application of the Fed. Bureau of Investigation*, 2013 WL 5741573, at *24–26.

126. *See, e.g.*, Jim Sensenbrenner, *NSA Abused Trust, Must Be Reined In*, MILWAUKEE J. SENTINEL (Nov. 2, 2013), http://archive.jsonline.com/news/opinion/nsa-abused-trust-must-be-reined-in-b99131601z1-230292131.html/ ("I led a bicameral group of legislators that came together and passed the USA [PATRIOT] Act with strong bipartisan support. . . . But the National Security Agency abused that trust. It ignored restrictions painstakingly crafted by lawmakers and assumed a plenary authority never imagined by Congress."). Sensenbrenner was, at the time this opinion piece was published, the chair of the House Judiciary

those steeped in the arcane details of foreign intelligence surveillance law—including the judges of the FISC—the program had appeared to fall within the boundaries set by the Constitution and law.[127] But the program was so unexpected that when its existence became publicly known, the outcry from civil libertarians, politicians, and many members of the public at large was swift and fierce.

The FAA 702 program, in contrast, followed a very different trajectory: although information about the program was also leaked by Edward Snowden, the activities carried out under the 702 program were tethered far more directly and predictably to clearly defined provisions of law and procedure.[128] The rationale for the program was explained in unprecedented detail at open hearings before Congress, as senior officials of the Intelligence community articulated why the mechanics of modern telecommunications infrastructure made it necessary to use access points within the United States to collect the communications of intelligence targets who were not U.S. persons and who were outside the U.S.[129] The language of the law, as ultimately passed and as subsequently amended, was clear in describing the intent of the law and providing predictability into

---

Committee's Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, and was one of the authors of the USA PATRIOT Act.

127. *See generally Strengthening Privacy Rights and National* Security, *supra* note 124 (testimony of Deputy Attorney General James Cole; Robert Litt, General Counsel of the Office of the Director of National Intelligence, and John C. Inglis, Deputy Director of the National Security Agency).

128. *See* PRIV. & C. L. OVERSIGHT BD., 113TH CONG., REP. ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 5 (2014).

129. *See, e.g.*, *Testimony of General Michael V. Hayden, Director, CIA, Before the S. Comm. on the Judiciary*, 109th Cong. (2006); *see also Hearing on the Protect America Act of 2007 Before the H. Permanent Select Comm. on Intel.*, 110th Cong. (2007) (statement of J. Michael McConnell, Director of National Intelligence); *Hearing on the Foreign Intelligence Surveillance Act and Implementation of the Protect America Act Before the S. Comm. on the Judiciary*, 110th Cong. 9 (2007) (statement of J. Michael McConnell, Director of National Intelligence); *Modernizing the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intel.*, 110th Cong. (2007) (statement of J. Michael McConnell, Director of National Intelligence). These, and other public statements and testimony during 2007, were focused on the specific FISA modernization proposal that would become the Protect America Act (PAA), a piece of federal legislation that temporarily authorized a legal framework to carry out foreign intelligence surveillance in a manner fundamentally similar to the program that would later become FAA 702. Because the PAA was set to sunset after only six months, Congressional passage of FAA 702 in 2008 was based in large part on the factual framework and policy justifications that had been put forward in 2007 during debate on FISA modernization and PAA. For more details on the history of the transition from the FISA Modernization Act to the PAA to FAA 702, *see generally* David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: A Working Paper of the Series on Counterterrorism and American Statutory Law* (Brookings Inst., Working Paper, 2007).

how it would be administered and applied.[130] Consequently, although the FAA 702 program has both supporters and critics, the debates have not, by and large, been sidetracked with concerns founded on unpredictability or surprise; instead, they focus where one might appropriately expect them to: on whether the statute's scope is sound policy, and whether courts ought to reconsider the long line of jurisprudence that has consistently found the program to be constitutional.[131]

More recently, a number of Trump-era uses of personal data have raised concerns that demonstrate the ways in which, even within a longstanding legal framework, the rise of new technologies continues to raise new questions about the scope of personal data by government actors. Examples include the practice of searching social media accounts as well as laptops, smartphones, and other devices at border crossing locations,[132] and the use of DNA testing for immigrants and refugees.[133] Historically, expanded search and surveillance activities at border crossings have been upheld, based on the reduced expectation of privacy and heightened governmental interests at international borders.[134] However, the increasingly expansive use of this authority by the Department of Homeland Security (DHS) has led to alarm,[135] and to litigation, as travelers protested the DHS policy of employing both "basic" and "advanced" searches, with advanced searches allowing officers to analyze, search, and copy the contents of electronic devices.[136] In one such

130. *See, e.g.*, PRIV. & C. L. OVERSIGHT BD., *supra* note 128, at 8–9 ("On the whole, the text of Section 702 provides the public with transparency into the legal framework for collection, and it publicly outlines the basic structure of the program.").

131. *See, e.g.*, *The Privacy Concerns at the Heart of the FISA Renewal Debate*, PBS NEWSHOUR (Jan. 11, 2018, 6:35 PM), https://www.pbs.org/newshour/show/the-privacy-concerns-at-the-heart-of-the-fisa-renewal-debate.

132. *See, e.g.*, HILLEL R. SMITH, CONG. RSCH. SERV., LSB10387, DO WARRANTLESS SEARCHES OF ELECTRONIC DEVICES AT THE BORDER VIOLATE THE FOURTH AMENDMENT? (2019).

133. *See, e.g.*, Abigail Hauslohner, *U.S. Immigration Authorities Will Collect DNA from Detained Migrants*, WASH. POST (Mar. 6, 2020, 2:59 PM), https://www.washingtonpost.com/immigration/us-immigration-authorities-will-collect-dna-from-detained-migrants/2020/03/06/63376696-5fc7-11ea-9055-5fa12981bbbf_story.html.

134. *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985) ("Consistently, therefore, with Congress' power to protect the Nation by stopping and examining persons entering this country, the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior. Routine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant, and first-class mail may be opened without a warrant on less than probably cause . . . . These cases reflect longstanding concern for the protection of the integrity of the border.") (footnote omitted).

135. *See, e.g.*, Carrie DeCell, *"Dehumanized" at the Border, Travelers Push Back*, KNIGHT FIRST AMEND. INST. (Feb. 2, 2018), https://knightcolumbia.org/content/dehumanized-border-travelers-push-back.

136. Alasaad v. Nielsen, No. 1:17-cv-11730-DJC, at 4 (D. Mass. Nov. 12, 2019).

case, *Alasaad v. Nielsen*, the plaintiffs were U.S. citizens or legal permanent residents who objected to Customs and Border Patrol (CBP) searches of the photos, contacts, social media, and other information that appeared on the travelers' electronic device. In that case, the federal district court held that, despite the border exception to the Fourth Amendment, officers must demonstrate reasonable suspicion prior to carrying out such searches.[137] In oral argument on appeal, the panel of First Circuit judges appeared skeptical of arguments that it ought to go beyond even the reasonable suspicion requirement found by the District Court and impose a requirement for individualized warrants for electronic device searches at the border, but at the time this article was being prepared for publication, no decision had yet been rendered in the matter.[138]

All of these policy debates are necessary to inform national security policy, as they have been in the law enforcement context, where courts have attempted to guide Fourth Amendment jurisprudence in a manner that keeps pace with changing technology.[139] However, there has been far less attention paid to the extraordinarily intrusive data collection, analysis, and behavioral prediction that is possible in the private sector. The term "surveillance capitalism" was coined as a catch-all phrase to encompass the many forms this takes.[140] This private sector scrutiny of our personal lives takes myriad forms and extends far beyond the social media environment and digital advertising contexts. It includes workplace demands that employees install location tracking apps on their personal

137. *Id.* at 38 (holding that "reasonable suspicion and not the heightened warrant requirement supported by probable cause . . . is warranted here").

138. Brian Dowling, *1st Circ. Wary of Border Phone Search Warrant Requirement*, LAW360 (Jan. 5, 2021, 3:01 PM), https://www.law360.com/articles/1341883/1st-circ-wary-of-border-phone-search-warrant-requirement; Andrea Vittorio, *Searches of Digital Devices Face Appeals Court Scrutiny*, BLOOMBERG L., https://news.bloomberglaw.com/privacy-and-data-security/border-searches-of-digital-devices-face-appeals-court-scrutiny-1 (Jan. 5, 2021, 2:58 PM).

139. Some of the most notable decisions arise in the context of Supreme Court decisions of the past twenty years. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (government acquisition of an individual's cell site location records constitutes a Fourth Amendment search); Riley v. California, 573 U.S. 373, 402 (2014) (police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested); United States v. Jones, 565 U.S. 400, 411 (2012) (continuous use of a GPS tracking device requires a warrant under the Fourth Amendment). However, digital data maintained by a third party does not fit neatly under existing precedents but lies at the intersection of two lines of cases, exemplified by GPS data privacy in *Jones* and the Third Party doctrine founded on United States v. Miller. 425 U.S. 435, 444 (1976) (no expectation of privacy in financial information held by a bank); Smith v. Maryland, 442 U.S. 735, 743–45 (1979) (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company).

140. *See generally* Mariano-Florentino Cuéllar & Aziz Z. Huq, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 133 HARV. L. REV. 1280 (2020).

phones, or wear RFID-enabled smart badges that track an employee's location through the workplace and even monitor the tone and volume of their voice when talking while wearing the badge.[141] It includes facial recognition technology being used in schools, and internet-enabled devices that can monitor and record the interactions of children in the classroom.[142] And of course it includes all of the ways that platforms that do not charge use fees rely on a business model which, at its heart, rests on monetization of user information. Despite these widespread uses, and the growing number of ways in which personal data can be used, or perhaps misused, by private actors, federal circuit courts remain split on the question of what facts are required in order for plaintiffs to have standing to sue for privacy-related claims in federal courts.[143] The Ninth Circuit, citing its own precedent as well as Third Circuit case law, noted that:

> advances in technology can increase the potential for unreasonable intrusions into personal privacy. . . . As the Third Circuit has noted, "[i]n an era when millions of Americans conduct their affairs increasingly through electronic devices, the assertion . . . that federal courts are powerless to provide a remedy when an internet company surreptitiously collects private data . . . is untenable. Nothing in *Spokeo* or any other Supreme Court decision suggests otherwise."[144]

VI. HOW CAN, OR SHOULD, THESE AREAS OF LAW INTERSECT?

What do these seemingly disparate threads have in common? All depend on the seemingly inexhaustible supply of personal data. The reforms, too, need to rest on a data-focused approach, one that recognizes that the convergence of technologies has inevitably led

---

141. DOSS, *supra* note 1, at 115–23.

142. *Id.* at 126–29.

143. *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 598 (9th Cir. 2020) ("[V]iolations of the right to privacy have long been actionable at common law.") (alteration in original) (quoting Patel v. Facebook, 932 F.3d 1264, 1272 (9th Cir. 2019)); *id.* ("A right to privacy 'encompass[es] the individual's control of information concerning his or her person.'") (alteration in original) (quoting Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017)) (internal citations omitted); *see also* Jason S. Wasserman, *Stand in the Place Where Data Live: Data Breaches as Article III Injuries*, 15 DUKE J. CONST. L. & PUB. POL'Y SIDEBAR 201, 202 (2020) ("Courts, however, do not even agree on whether or when data breach victims can sue, or in other words, when the victims suffer cognizable legal injuries that create Article III standing.").

144. *In re Facebook, Inc. Internet Tracking*, 956 F.3d at 599 (alterations and omissions in original) (citing *Patel*, 932 F.3d at 1272 and *In re* Google Inc. Cookie Placement Consumer Priv. Litig., 934 F.3d 316, 325 (3d Cir. 2019)).

to an intersection of ills—and those ills can best be addressed through intersecting approaches to law and policy.

Each of these issues—consumer data privacy, national security, domestic terrorism, speech, platform liability protections—are complex in their own right. Combining them into a single framework for analysis and potential solutions might seem to be a fool's errand—a combination that, by including more dimensions, makes the puzzle infinitely more complex. It is more likely, however, that the opposite is true: the puzzle is already complex and multi-faceted, regardless of whether we choose to acknowledge or leverage the interrelatedness of these issues. The irreducible fact is that significant dimensions of each of these problems already intersect in ways that we cannot unravel.

To put it another way: we are often treating each of these major areas of legal uncertainty and evolving legal doctrine as if they are separate, standalone jigsaw puzzles; if only we can find pieces of the right shape and color, and orient them in the right way, we can solve the puzzle of consumer data privacy, or election-related information operations, or national security surveillance, or platform liability for speech or online harms, or antitrust implications of technology providers, bringing each of these disparate areas into focus as a clear and coherent two-dimensional picture, with each completed puzzle resting on its own table, on its own puzzle mat, having been worked by an independent team of advocates, experts, and practitioners who are steeped in that particular set of issues. This approach, however, is likely as outdated as the analog paper storage and retrieval mechanisms that have largely been replaced by digitized, complex, data and algorithms. In our interconnected, digital ecosystem, in which personal information underpins so many seemingly disparate actions and interactions, the problem set is no longer a library of independent two-dimensional jigsaw puzzles, each of which can be solved on its own. Instead, they are more like a Rubik's cube: trying to solve one side of the puzzle in isolation from the others does nothing to move towards an overall scheme—in fact, the opposite is true, since solving for one side hopelessly scrambles the cube's other five surfaces, making them less coherent than before. The only way to solve the Rubik's cube and align its colors is to solve for all six of its sides at once, knowing that in the process there may be times when the tension between sides—the impact of one set of moves on the other surfaces—at first appears to be counterproductive, but is a necessary accommodation to consider in order to reach the end-state solution.

Privacy rights, civil liberties, technology innovation, freedom of speech, and national security are all, of course, weightier issues by far than aligning colors on a Rubik's cube; it is no surprise that the analogy is an imperfect one, and it particularly breaks down when it comes to sacrificing important interests in one sphere of law in order to optimize another. So while scrambling one side of a Rubik's cube to solve the overall puzzle is an easy decision to make, policymakers and privacy advocates alike ought to avoid situations in which one side of the multidimensional data puzzle gets scrambled in an effort to make gains on another side.[145] With the significance of different policy choices top of mind, the list below provides a modest selection of ways that policymakers and legislators can go about addressing the interrelated bundle of issues that form distinct but interrelated parts of this multidimensional personal data puzzle.

A. Acknowledge the Convergence of Technology—and Embrace Cross-Pollination of Legal Theories

During the FISA modernization hearings of 2007, a frequent refrain was technology convergence, and the ways in which the internet and twenty-first century telecommunications raised new challenges: intelligence targets were using the same free webmail services, internet forums, and other modes of communication used by ordinary people in the U.S. and around the world, and an ever-more-pressing challenge of intelligence gathering was separating out the signal from the noise, of finding the terrorist communication among the proliferation of cat videos. That challenge has only grown more acute in the years since then, as social media, encrypted messaging, mobile advertising, personal data profiles, mobile apps, Internet of Things devices, and more become a ubiquitous part of everyday life, and as companies maintain storehouses of

145. This is arguably what has resulted from the European Union's decisions over the years to tie permission for international transfer of commercial data to its concerns about U.S. national security activities. In the *Schrems II* decision, the CJEU invalidated the Privacy Shield framework and cast doubt on the future viability of standard contractual clauses—key mechanisms supporting the transfer of personal data. However, the impact—the cost, burden, limitations on commerce, etc.—of this decision falls on private sector entities who have no ability to influence U.S. surveillance law. While it is conceivable that the U.S. Congress might at some point structure U.S. intelligence gathering activities in ways that satisfy European courts and privacy advocates, it is not at all clear that that's the case, for a great many reasons not discussed here. The end result is that a European privacy regulation has been interpreted in such a way as to scramble the international commerce side of the Rubik's cube in hopes that the resulting pressure will force the U.S. to solve the national security side of the puzzle in a way that is to the EU's liking. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems, 2020 E.C.R. I-559.

data on individuals that dwarfs anything held by governments, including by national security and law enforcement agencies in the U.S.

Proposals for reform of Section 230's liability protections, new legal theories relating to content moderation, and discussions of government purchases of commercially available information that forms part of the digital advertising market should all be considered in the overall context of surveillance law, consumer data privacy, and cybersecurity obligations and data breach notification laws.

B. Expand Data-Related Regulations on the Private Sector

With the inauguration of a new administration, policy recommendations abound, as think tanks, civil society groups, and others offer comments on ways that the federal government can consider addressing the most pressing issues associated with personal data and technology platforms.[146] Proposals for a federal data privacy law have circulated for years; the 117th Congress presents a unique opportunity to capitalize on that momentum by passing a comprehensive data privacy law that would impose minimum principles and standards for handling of personal information. If privacy legislation includes obligations of transparency and mechanisms for oversight and redress of violations, then private sector use of information can be removed from the current landscape, in which individuals are often out-leveraged by large corporations and placed on a more equal footing with the more highly regulated uses of information by government actors.

C. Level the Playing Field in Government Regulations

One of the issues that has become apparent is that there is no uniform set of standards, regulations, procedures, or approaches governing the activities of local, state, and federal agencies that handle personal information. Whether government entities acquire data directly, through mechanisms like government-operated street

146. *See, e.g.*, April Falcon Doss, *Data and Democracy: Three Things the Biden-Harris Administration Should Do to Tackle Big Tech*, JUST SEC. (Nov. 30, 2020), https://www.justsecurity.org/73538/data-and-democracy-three-things-the-biden-harris-administration-should-do-to-tackle-big-tech/; Alexandra Reeve Givens, *CDT Recommendations to the Biden Administration and 117th Congress to Advance Civil Rights & Civil Liberties in the Digital Age*, CDT (Jan. 20, 2021), https://cdt.org/insights/cdt-recommendations-to-the-biden-administration-and-117th-congress-to-advance-civil-rights-civil-liberties-in-the-digital-age/; India McKinney & Ernesto Falcon, *EFF's Top Recommendations for the Biden Administration*, EFF (Jan. 21, 2021), https://www.eff.org/deeplinks/2021/01/effs-top-recommendations-biden-administration.

cameras or surveillance drones, or indirectly, by obtaining it from private sector data collectors, it is essential for government departments and agencies to provide transparency about their data practices, and for those practices to be subject to robust and effective oversight mechanisms. While state and local government uses of data will continue to be a matter for state and local control, the federal government can and should assess government-wide use of data and look to level the playing field of federal government regulations and oversight where gaps currently exist.

D. Prioritize Education and Public Awareness Campaigns

Providing improved digital literacy education and public awareness campaigns is becoming an increasingly vital need. Focusing on media literacy and related topics in schools is important but insufficient; research has shown that older Americans are more susceptible to online disinformation than younger ones.[147] With that dynamic in mind, outreach could include measures like traditional producing television-format public service announcements intended to reach older Americans who watch television and who also may be prone to sharing misinformation on their Facebook feeds. Separate lines of research have shown that librarians consistently are viewed as highly trusted sources of reliable information[148] and may be able to play a key role in combatting online disinformation—although resources and other constraints currently pose challenges.[149]

Sound policy proposals for combatting online disinformation abound.[150] These proposals should be given serious consideration, tried, and then tested for efficacy, and then expanded upon.

---

147. *See, e.g.*, *Troll Watch: Study Shows Older Americans Share the Most Fake News*, NPR (Jan. 13, 2019, 5:21 PM), https://www.npr.org/2019/01/13/684994772/troll-watch-study-shows-older-americans-share-the-most-fake-news.

148. A.W. Geiger, *Most Americans—Especially Millennials—Say Libraries Can Help Them Find Reliable, Trustworthy Information*, PEW RSCH. CTR. (Aug. 30, 2017), https://www.pewresearch.org/fact-tank/2017/08/30/most-americans-especially-millennials-say-libraries-can-help-them-find-reliable-trustworthy-information/.

149. *See, e.g.*, Suzanne LaPierre, *New Research Explores How Public Libraries Can Best Combat Misinformation*, PUB. LIBR. ASS'N (Nov. 23, 2020), http://publiclibrariesonline.org/2020/11/new-research-explores-how-public-libraries-can-best-combat-misinformation/.

150. *See, e.g.*, Nina Jankowicz, *How to Defeat Disinformation: An Agenda for the Biden Administration*, FOREIGN AFFS. (Nov. 19, 2020), https://www.foreignaffairs.com/articles/united-states/2020-11-19/how-defeat-disinformation.

E. Empower Congressional Oversight with Cross-Committee Jurisdiction

The range of legal and social issues stemming from data-driven technologies currently spans multiple committees in both houses of Congress.[151] Adopting a model that supports robust cross-committee jurisdiction will help advance opportunities for sensible cross-pollination of ideas.[152]

F. Assess the Need for Additional Independent Oversight Bodies

Government entities at local, state, and federal levels are all subject to Constitutional constraints[153] and are typically subject to some form of political control,[154] transparency obligations,[155] and independent oversight, which may be carried out by courts, by inspectors general, by independent commissions, or by other duly authorized bodies. Even where the public is not afforded direct access to information about data collection or handling—such as in the national security context, in which many government programs are classified and information about them is therefore tightly controlled—there frequently exists some set of overseers who have been granted authority to review all pertinent information regarding a program or activity and stand in the shoes of the people for purposes of scrutinizing the lawfulness and prudence of the programs at issue.[156]

Private entities, however, lack these mechanisms. Their status as private entities means they are only subject to the particular controls that might apply to their specific industry (such as OCR's

151. *See generally* Doss, *supra* note 121.

152. *See generally id.*

153. In the case of state and local government entities, those constraints may be heightened by the provisions of state constitutions as well as state statutes or local ordinances that impose additional privacy and speech protections that are conferred by the U.S. Constitution.

154. Political control may come from voters as well as from a legislative branch of government at the federal, state, or local level—whether it be by Congress or a City Council, executive branch agencies at federal, state, and local levels are generally subject to legislative scrutiny as well as mechanisms for accountability to the people they serve.

155. Through federal laws, such as the Privacy Act and Freedom of Information Act, federal agencies are required to provide transparency into a variety of government activities relating to the use of personal information. All fifty states have some form of freedom of information or open records legislation, and some local government entities have additional transparency requirements. *See, e.g.*, *State Freedom of Information Laws*, NAT'L FREEDOM INFO. COAL., https://www.nfoic.org/coalitions/state-foi-resources/state-freedom-of-information-laws (last visited Feb. 15, 2021).

156. In the national security context, these overseers include the U.S. House and Senate intelligence committees, the Foreign Intelligence Surveillance Court, the Privacy and Civil Liberties Oversight Board, and the inspectors general of all of the departments and agencies that comprise the U.S. intelligence community.

authority to carry out investigations of HIPAA covered entities) or status (such as the SEC's authority to carry out investigations into certain activities of publicly traded companies). Consumers have only a limited ability to pressure companies into providing greater transparency or accountability—particularly when the company holds a dominant market share for a particular good or service, leaving consumers with few alternative providers; companies that recognize the inherent power created by holding a dominant market position may feel little incentive to respond to consumer concerns, whether those relate to personal data privacy, algorithmic functions and bias, content moderation policies, data sharing practices, or other aspects of a company's operations and use of personal information. This transparency can, however, be significantly bolstered through a regulatory framework of the type noted in Section II, above. The FTC has long made use of its Section 5 authority to create a sort of regulatory bootstrapping: where a company was initially subject only to general obligations to refrain from unfair or deceptive acts or practices, a company that has entered into a consent decree with the FTC is frequently subject thereafter to very specific obligations, and any failure to comply could result in fines or other regulatory consequences for failing to abide by the terms of the consent agreement. A more direct approach would be to create specific regulatory obligations in federal legislation governing data privacy, security of personal information, and other key areas at the intersection of personal data and pressing policy concerns. Such a regulatory framework could expand the staffing, authority, and role of the FTC, or create one or more new regulatory bodies to carry out investigations and oversight. It could require regular transparency reporting of the kind currently required for the intelligence community.

VII. CONCLUSION

As the online ecosystem grows ever more complex, so do the intersections among previously-disparate fields of law. Consumer data privacy and national security are two areas in which these intersections have become particularly striking. Antitrust, transparency of election-related advertising and other paid political content, and the ongoing need for Fourth Amendment jurisprudence in the law enforcement context are, as briefly alluded to above, other areas of law that strain to keep pace with the critical intersections between new technologies and the many ways in which personal information can be created, collected, collated, manipulated,

organized, analyzed, assessed, sold, shared, and more. As legislators, policymakers, advocacy groups, and academics continue assessing how law can be used as a tool of public policy to protect individual rights, protect national security, and preserve domestic tranquility, their chances of arriving at successful approaches goes up if these challenges are treated like the intersecting faces of a Rubik's cube, rather than confined to separate "cylinders of excellence."