Journal of Business & Technology Law

Volume 15 | Issue 1 Article 2

Time for a New Tech-Centric Church-Pike: Historical Lessons from Intelligence Oversight Could Help Congress Tackle Today's Data-Driven Technologies

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

APRIL FALCON DOSS*©

INTRODUCTION

In the 1970s, Congress undertook a significant restructuring of its approach to overseeing surveillance carried out by the U.S. intelligence community. A series of scandals, combined with accidental revelations and public concern, led leaders in the United States House and Senate to recognize that the existing Congressional committees were not well situated to make policy assessments, carry out oversight, or draft and propose new legislation relating to surveillance activities by the United States. Some of the gaps Congress experienced were created by emerging technologies. Many of the gaps related to more prosaic issues of turf: which committees controlled which budgets, which committees had members with an inherent interest in particular topics, and which topics had generated congressional oversight in the past. But Congress was also attempting to grapple with what had been revealed as a sprawling challenge: how to ensure Congress had visibility into the vast scope of governmental intelligence activities, and how to appropriately constrain those activities in order to balance the necessary and appropriate interests in national security with the protection of the rights and liberties vital to a functioning democracy. When Congress passed the resolutions forming the two committees that would take up this challenge, Congress recognized that existing committees simply did not have the breadth of jurisdiction, depth of staff, or other practical resources required in order to effectively tackled such a complex and sprawling challenge.[1]

---

* April Falcon Doss is currently a partner and chair of the Cybersecurity and Privacy practice at the law firm Saul Ewing Arnstein & Lehr. Prior to that, she served on as Senior Minority Counsel for the Russia Investigation in the United States Senate Select Committee on Intelligence, and as Associate General Counsel for Intelligence Law at the National Security Agency. She is adjunct faculty at the University of Maryland Carey Law School, where she teaches courses on Information Privacy and Internet Law.

1. The House of Representatives passed H.R. Res. 591, which "Established in the House of Representatives a Select Committee on Intelligence to conduct an inquiry into the organization, operations, and oversight of the

Those two committees, informally referred to as the Church and Pike Committees after their respective chairmen in the U.S. Senate and House of Representatives, focused on activities of the executive branch of government. Notwithstanding the specific focus of those historical committees, there are useful parallels between the challenges faced by Congress prior to establishing the Church and Pike committees and the challenges faced by Congress in dealing with data-driven technologies today. Given the complexity of issues prompted by current technology developments, it is unlikely that any single solution will be sufficient to effectively and comprehensively resolve the full scope of legal and policy questions that need to be addressed in the data-intensive world in which we all live. Nonetheless, establishing special bipartisan committees in both houses of Congress, committees whose jurisdiction is designed to cut across existing committee lines and encompass a wide scope of issues arising from the impact on individuals and society of data-driven technologies, could be one important tool in supporting the ability of American law and policy to keep pace with the rapid rate of technological change.

At first blush, these committees might seem like an odd comparison. After all, the intelligence committees were established to oversee executive branch activity, not to delve into the widespread array of knotty legal and policy questions that arise from matters that necessarily includes private sector collection and use of information about individuals. Further, the intelligence committees were established with what might have appeared to be a clearer foundation of national principles, principles which should serve as a yardstick for measuring the activities of private companies' actions. That is to say, longstanding Constitutional principles enshrined in the First and Fourth Amendments and long-held commitments to democracy and self-determination, as well as important interests of foreign affairs and national security, were implicated in identifying an appropriate balance between intelligence collection and individual liberty and national self-determination. Given that many of the most innovative uses of data-intensive technology today are arising within the private sector, rather than from government action, the source of authority to legislate in those areas will not, in all instances, arise from Constitutionally-protected interests as was the case for the intelligence activities overseen by the Church and Pike committees.

Upon closer inspection, however, the current challenges in assessing how to maintain individual privacy and liberties against a backdrop of widespread private sector collection, aggregation, analysis, and use of personal information bear striking similarities to the challenges faced by Congress and the American public in the 1970s. In other words, although the specifics differ, many common

---

intelligence community of the United States Government." H.R. Res. 591, 94th Cong. (1975). The Senate counterpart to this action was S. Res. 21, a "Resolution to establish a select committee of the Senate to conduct an investigation and study with respect to intelligence activities carried out by or on behalf of the Federal Government." S. Res. 21, 94th Cong. (1975).

characteristics exist. Then, as now, technological advances had made it possible to collect more detailed information about individuals than had ever been possible before, and once collected, to use that information in more wide-ranging ways, from creating personal behavioral profiles to attempting to sway individuals' opinions and actions.

In the 1970s, these expanded capabilities to collect, combine, and use data in novel ways, raised widespread concerns about government surveillance and privacy-intrusive activities ultimately prompting Congress to establish the first select intelligence committees. The Church and Pike committees were endowed with investigative and oversight authorities that made them uniquely well postured to carry out thorough and wide-ranging analysis of the multiple problems that confronted them. The impact of their hearings and recommendations formed critical and effective parts of the long-term framework for overseeing government intelligence activities which still remain in place today.

Today, data-intensive technologies have vastly increased the capacity for detailed information about individuals and groups to be collected, combined, and used in novel and ever-expanding ways. While the Congressional intelligence committees continue to oversee the government's use of that data for foreign intelligence purposes, much of the most innovative, and intrusive, new data-intensive capabilities are being developed and deployed by the private sector, not by government. With this evolution in mind, the historical example of the Church and Pike Committees provide an example of how Congress could take a similar, although not identical, approach and fashion select bipartisan, bicameral Congressional committees focused on policy and legislative issues arising from data-driven technology. If properly constructed, these committees could play a significant role in identifying the scope of public concern, advancing the scope of appropriate legislation, influencing the course of executive action, and providing guidance for emerging jurisprudence on data-driven issues affecting individual privacy and other important rights and equities.

I. PRECEDENT FOR ESTABLISHING NEW CONGRESSIONAL COMMITTEES

Congressional committees come and go. By various counts, there have been some 1,500 Congressional committees formed and disbanded over the course of the nation's history.[2] Many of these are established for a specific investigative purpose, such as the Select Committee on the Assault on Senator Sumner, which was

2. *See, e.g.*, WALTER STUBBS, CONGRESSIONAL COMMITTEES, 1789-1982: A CHECKLIST VII (1985); 4 ROBERT C. BYRD, THE SENATE: 1789-1989 HISTORICAL STATISTICS 1789-1992 513–15 (1993); CHARLES E. SCHAMEL ET AL., GUIDE TO THE RECORDS OF THE U.S. HOUSE OF REPRESENTATIVES AT THE NATIONAL ARCHIVES, 1789-1989 289 (1989); DAVID T. CANON, GARRISON NELSON & CHARLES STEWART III, COMMITTEES IN THE U.S. CONGRESS: 1789-1946 SELECT COMMITTEES (CQ Press vol. 4 2002).

established in 1853 and expired in 1856.[3] Others were established to consider a particular issue, such as special committee on the Atmospheric Telegraph Between Washington and Baltimore, an 1854 proposal considered in the U. S. Senate for the construction of a pneumatic tube that would allow conveyance of communications between the two cities.[4] Others have related to specific time-bounded events, such as the special committee on the "Year 2000 Technology Problem."[5] Still others have been triggered by politically-motivated oversight needs, such as the review of campaign expenditures in 1924 and 1932, or the many investigations in the early 2000s into the terrorist attack on the U.S. Embassy in Benghazi.[6]

On occasion, however, specially designated or select committees, established to address a specific problem, concern, or interest or a specific time, garner strong bipartisan support and demonstrate sustained usefulness that they become institutionalized as part of long-term reforms. These committees shape how lawmakers approach the thorny problems associated with particular topics which, are acute in nature at a particular time, but also take on enduring importance. It's the contention of this paper that the House and Senate Select Committees on Intelligence are among these examples, and that, despite the deep and noteworthy shortcomings in their operations over the years, the enduring record of these two committees provides important lessons as well as a useful model for today, as lawmakers struggle to understand the ways in which data-driven technologies are reshaping modern society, and to consider ways in which legislation might help address those concerns.

The times in which these committees were formed, and the challenges they faced, were no less pressing than those faced by Congress today. The challenges inherent in making appropriate policy decisions regarding data-driven technologies today cover a landscape of issues that are broader than those which confronted the Church and Pike committees in the 1970s. There are nonetheless useful parallels in the challenges associated with deciding whether and how to investigate, support, oversee, legislate, and interact with the multiplicity of stakeholders whose activities and equities must be addressed if Congress is to have any hope of tackling modern data issues in a holistic fashion. Despite the differences, described in more detail below, a number of situational similarities remain. These two committees were first established in the 1970s against a backdrop of particularly fraught partisan

3. *Assault of Charles Sumner*, HISTORY, ART & ARCHIVES, U.S. H.R., https://history.house.gov/Records-and-Research/Listing/hi_003/ (last visited Sept. 14, 2019).

4. 31 WILLIAM B. DANA, MERCHANTS' MAGAZINE AND COMMERCIAL REVIEW (New York, 142 Fulton Street 1854). 31 FREEMAN HUNT A.M., HUNT'S MERCHANT MAGAZINE AND COMMERCIAL REVIEW 266 (New York, 142 Fulton Street 1854).

5. *See generally,* S. Res. 208, 105th Cong. (1998) (enacted).

6. 4 DAVID T. CANON, GARRISON NELSON & CHARLES STEWART III, COMMITTEES IN THE U.S. CONGRESS: 1789-1946 SELECT COMMITTEES 755 (2002) (committee to investigate the 1924 campaign expenditures); S. REP. NO. 73-191, at 1 (1934) (committee to review presidential and senatorial campaign expenditures in 1932); H.R. REP. NO. 113-442, at 1–2 (2014) (committee to review the Benghazi attack in 2000).

concern. They were established to address questions that Democrats and Republicans viewed through strikingly different partisan lenses.

II. THE PROBLEMS THAT CHURCH AND PIKE SOUGHT TO INVESTIGATE

In 1975, Senator Frank Church from Idaho dropped the gavel on proceedings that would fundamentally reshape intelligence activities by the U.S. government for the next half-century to come. His counterpart, Otis G. Pike, in the U.S. House of Representatives did the same. And although Pike's Committee would never issue a final report, the hearings held by both of these specially appointed, bipartisan Congressional committees led to unprecedented transparency on the scope of U.S. intelligence activities. The record they created through documentary evidence, witness testimony, and staff-generated recommendations led to new statutes, new executive orders, new oversight mechanisms, and even to an entirely new federal court with its own unique set of procedural rules, staff, and secure hearing location. The Church and Pike Committees were established by Congress as temporary mechanisms; special select committees to examine the urgent, pressing concerns facing the nation about the conduct of intelligence activities that affected U.S. persons.[7] Part of the reason why they were necessary was that, up until that time, there was no single set of committees with jurisdiction over the activities of the agencies and departmental components that had become the U.S. intelligence community.[8] Without direct-line oversight functions being exercised in Congress, and with some intelligence activities falling either outside the boundaries of Congressional oversight or falling between the jurisdictional cracks of different committees, it was all too easy for intelligence gathering functions to be carried out in a manner that escaped meaningful external scrutiny altogether. This problem of oversight was compounded by the fact that intelligence activities fell outside the purview of the courts, and – for obvious reasons – were nearly always conducted in secrecy.[9]

---

7. See A Resolution establishing a Select Committee on Intelligence, H. RES. 138, 94th Cong. (1975) (enacted); H.R. RES. 591, 94th Cong. (1975); S. RES. 21, 94th Cong. (1975).

8. For example, the House had an Armed Services Committee which had authority to oversee and investigate activities of the armed forces, but whose authority did not extend to CIA or the FBI. The Judiciary Committee had jurisdiction over the Department of Justice and, with it, FBI, but had no authority over agencies such as NSA or DIA. The Committee on International Relations might be concerned about the impact that covert operations could have in foreign relations. None of these committees, however, was empowered to oversee all of the activities engaged in by the Intelligence Community. See *Calendars of the United States House of Representatives and History of Legislation*, 94th Cong., 4, https://library-clerk.house.gov/reference-files/House_Calendar_94th_Congress.pdf. *See also* S. REP. NO. 94-755, Book II at III–IV. In that letter, Sen. Church wrote that "The root cause of the excesses which our record amply demonstrates has been failure to apply the wisdom of the constitutional system of checks and balances to intelligence activities." *Id.*

9. In its Conclusions, the Church committee wrote that, "For decades Congress and the courts as well as the press and the public have accepted the notion that the control of intelligence activities was the exclusive prerogative of the Chief Executive and his surrogates. The exercise of this power was seen as flowing not from

The Watergate break-in of 1972, the Watergate hearings of 1973, and President Nixon's resignation in 1974 had all paved the way for a deep mistrust of the executive branch of government. The country – divided over so many domestic and foreign policy issues, from civil rights to the Vietnam war – was keenly burdened with a sense of the risks that were possible when government went unchecked. And a series of recent investigations had suggested that the U.S. Intelligence Community might indeed have gone far too unchecked for too long.

A series of hearings and reports[10] had brought to light a string of allegations about CIA assassination plots directed at the heads of states of other countries, and had raised questions about domestic spying on Americans by the CIA, as well as CIA covert action programs overall.[11] Who, if anyone, was keeping an eye on the activities of intelligence agencies that had been operating with relatively little Congressional scrutiny in the decades since World War II? It wasn't just the CIA and covert action, however. Military departments and their intelligence components were alleged to have sent military intelligence officers to infiltrate activist groups.[12]

---

the law, but as inherent in the Presidency. Whatever the theory, the fact was that intelligence activities were essentially exempted from the normal system of checks and balances." *Id.* at 292. This view is supported by the language of Supreme Court opinion Katz v. U.S., noting that the court's finding that the Fourth Amendment applied to electronic surveillance even in the absence of a physical trespass was a holding limited to the law enforcement context. The court wrote that, "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Katz v. United States*, 389 U.S. 347, 358 n. 23 (1967). Similarly, the legislative history for the Foreign Intelligence surveillance Act noted that, "The history and law relating to electronic surveillance for "national security" purposes have revolved around the competing demands of the President's constitutional powers to gather intelligence deemed necessary to the security of the nation and the requirements of the fourth amendment. The U.S. Supreme Court has never expressly decided the issue of whether the President has the constitutional authority to authorize warrantless electronic surveillance for foreign intelligence purposes. Whether or not the President has an "inherent power to engage in or authorize warrantless electronic surveillance and, if such power exists, what limitations, if any, restrict the scope of that power, are issues that have troubled constitutional scholars for decades." H.R. REP. NO. 95-1283, at 15.

10. *See, e.g.*, "The recurring need for reexamining the way Congress monitors the activities of the intelligence agencies was again highlighted during the investigation in 1973 of the Senate Select Committee on Presidential Campaign Activities when questions were raised about the legality or propriety of certain intelligence activities of the CIA, the FBI, and other agencies." S. REP. 94-675, at 4 (accompanying S. RES. 400. 95th Cong. (1975)). "Allegations that the CIA had been involved in plans to assassinate certain leaders of foreign countries came to the Commission's attention shortly after its inquiry was under way." *Id.* at xi.

11. "One of the main controversies raised by recent practices of the Central Intelligence Agency is the question of intelligence collection about Americans. Unlike the FBI, the CIA was intended to focus on foreign intelligence matters. Charges have been made, however, suggesting that the CIA spied on thousands of Americans and maintained files on many more, all in violation of its statutory charter." S. REP. NO 94-755, Book III at 681.

12. "Although they are not expressly authorized by law, each of the military services investigates civilian groups, both within and without the United States, which it considers "threats" to its personnel, installations, and operations. In the late 1960s, all of the services were engaged in monitoring civilian antimilitary groups within the United states . . . Most of the information gathered about these antimilitary

From newspaper reports to Congressional hearings, a series of revelations had revealed a seemingly endless string of tales about U.S. intelligence agencies infiltrating civil rights and anti-war groups, and spying on Americans from Dr. Spock to Dr. Martin Luther King.[13]

In response to these snowballing allegations, in January of 1975, a newly re-constituted Senate, with a Democratic majority arriving in Washington fresh from the 1974 election, passed Senate Resolution 21,[14] establishing the Committee that would be run by Idaho Senator Frank Church, and formally granted the jurisdiction to investigation the actions of the U.S. Intelligence Community.[15] The U.S. House of Representatives established a similar inquiry, a special committee which was created in February, 1975. Colloquially known as the "Pike Committee," after Representative Otis Pike of New York, the Democrat who had been tapped to chair it, this early attempt at House oversight of U.S. intelligence activities never quite got its bearings. Distracted by the resignation of its original chair and mired in a series of battles with Gerald Ford's administration over what information the CIA would and would not produce, the Pike Committee's work was never officially released, although bootleg copies of its report were leaked to various outlets and found their way into publication in the U.S. and overseas.[16]

It was against this backdrop of concerns that had been growing in the political consciousness of the country that the Church and Pike Committees' investigations into domestic intelligence activities were launched. On January 21, 1975, Senate Resolution 21 was introduced, calling for the establishment of a select committee to investigate federal intelligence operations and determine "the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the

---

groups was collected from law enforcement agencies and the news media, but the services also quite commonly inserted their own undercover agents and informants into the groups." *Id.* at 790.

13. *See, e.g.*, *Ex-Officer Says Army Spies on Civilian Activities*, N.Y. TIMES (Jan. 16, 1970), https://www.nytimes.com/1970/01/16/archives/exofficer-says-army-spies-on-civilian-activists-1000.html; Seymour Hersh, *Huge CIA Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES (Dec. 22, 1974) https://www.nytimes.com/1974/12/22/archives/huge-cia-operation-reported-in-u-s-against-antiwar-forces-other.html; Ian Shapiro *He was America's most famous pediatrician. Then Dr. Spock attacked the Vietnam Draft.*, WASH. POST (Jan. 5, 2018), https://www.washingtonpost.com/news/retropolis/wp/2018/01/05/he-was-americas-most-famous-pediatrician-then-dr-spock-attacked-the-vietnam-draft/.

14. S. RES. 21, 94th Cong. (1975).

15. "Resolved, to establish a select committee of the Senate to conduct an investigation and study of governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government or by any persons, acting individually or in combination with others, with respect to any intelligence activity carried out by or on behalf of the Federal Government." *Id.*

16. *See, e.g.*, *Pike Charges CIA Effort at Retaliation for Findings,* N.Y. TIMES (Mar. 10, 1976), https://www.nytimes.com/1976/03/10/archives/pike-charges-cia-effort-at-retaliation-for-findings-accuses-agency.html; *see also* Gerald K. Haines, *The Pike Committee Investigation and the CIA: Looking for a Rogue Elephant*, CIA (last updated June 7, 2008), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/winter98_99/art07.html.

Federal Government."[17] The Resolution laid out a number of specific questions for the Committee's inquiry. These included an investigation into whether the CIA had carried out illegal domestic intelligence operations; a review of the scope of domestic intelligence or counterintelligence activities against U.S. citizens by the FBI or other agencies of the Intelligence Community; the state of cooperation across the IC, and what role those interagency dynamics may have had in illegal activity; the nature and extent of Executive Branch oversight of intelligence activities and the need for increased Congressional oversight of IC activities; whether there needed to be specific legislative authorization for agencies such as NSA and DIA which didn't have a statutory underpinning; and a list of additional enumerated questions as well as a catch-all authority to investigate such other and further questions as might arise during the course of the Committee's review.[18] The Senate approved the resolution, 82-4.[19]

As would be the case for every intelligence oversight committee moving forward, many of the Committee's hearings were held in closed session due to the classified nature of much of their review. However, in the fall of 1975, a series of lengthy public hearings was conducted as well. The Committee held 126 full committee meetings, 40 subcommittee hearings, interviewed approximately 800 witnesses (some in public and many in closed sessions), and reviewed 110,000 documents. Its final report, containing 96 specific recommendations, was published in April 29, 1976.[20] Importantly, this is a scope of work that would have almost certainly been impossible had it not been for the creation of a select committee, with subpoena power, staff, and a mandate to carry out this work.

The Committee was well aware of the historic nature of its work, noting as it did at the very outset of its report, that this was the first comprehensive review of U.S. intelligence activities to take place since World War II.[21] The Committee wrote that:

> This final report provides a history of the evolution of intelligence, an evaluation of the intelligence system of the United States, a critique of its problems, recommendations for legislative action and recommendations to the executive branch. The Committee believes that its recommendations will provide a sound framework for conducting the vital intelligence activities of the United States in a manner which meets the nation's intelligence requirements and protects the liberties of

17. S. RES. 21, 94th Cong. (1975) (enacted).

18. *Id.*

19. *S. Select Comm. To Study Governmental Operations with Respect To Intelligence Activities*, UNITED STATES SENATE, https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm (last visited Sept. 12, 2019).

20. *Id.*

21. S. REP. NO. 94-755, Book I, at 1 (1976).

> American citizens and the freedoms which our Constitution guarantees.[22]

The committee took pains to balance the legitimate needs for intelligence gathering with the vital interests of liberty. In doing so the committee recognized that "an extensive national intelligence system has been a vital part of the United States government since 1941. Intelligence information has had an important influence on the direction and development of American foreign policy and has been essential to the maintenance of our national security."[23] The Committee provided a devastating summary critique:

> Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. Investigations of groups deemed potentially dangerous-and even of groups suspected of associating with potentially dangerous organizations-have continued for decades, despite the fact that those groups did not engage in unlawful activity. Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. Unsavory and vicious tactics have been employed-including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform. Governmental officials-including those whose principal duty is to enforce the law-have violated or ignored the

22. *Id.*
23. *Id.*

> law over long periods of time and have advocated and defended their right to break the law.[24]

The authors of the report laid the blame at the feet of all three branches of government, noting that each had failed in some part of its duty to secure liberty along with security.

> The Constitutional system of checks and balances has not adequately controlled intelligence activities. Until recently the Executive branch has neither delineated the scope of permissible activities nor established procedures for supervising intelligence agencies. Congress has failed to exercise sufficient oversight, seldom questioning the use to which its appropriations were being put. Most domestic intelligence issues have not reached the courts, and in those cases when they have reached the courts, the judiciary has been reluctant to grapple with them.[25]

Although the Church and Pike committees focused on activities of the U.S. government, it is clear that there are parallels with the issues raised by private sector data collection today. At the most foundational conceptual level, the Church committee was concerned about the ways that expansive information-gathering, and the follow-on uses of that information, intruded on individual privacy and chilled the exercise of Constitutionally protected rights. In the Committee's words, "Personal privacy is protected because it is essential to liberty and the pursuit of happiness."[26] Further elaborating on this concern, the Committee noted that "our Constitution checks the power of Government for the purposes of protecting the rights of individuals, in order that all our citizens may live in a free and decent society. Unlike totalitarian states, we do not believe that any government has a monopoly on truth."[27] They went on to state:

> Since the end of World War II, governmental power has been increasingly exercised through a proliferation of federal intelligence programs. The very size of this intelligence system multiplies the opportunities for misuse.
>
> Exposure of the excesses of this huge structure has been necessary. Americans are now aware of the capability and proven willingness of their Government to collect intelligence about their lawful activities and associations. What some suspected and others feared has turned out to be largely true – vigorous expression of unpopular views, association

24. S. REP. NO. 94-755, Book II, at 1, 5–6 (1976).
25. *Id.* at 6.
26. S. REP. NO 94-755, Book II, at 290.
27. *Id.* at 290–91.

> with dissenting groups, participation in peaceful protect activities, have provoked both government surveillance and retaliation.[28]

Had the Committee's report focused on the impact of large-scale private sector data collection of information about individuals, and the subsequent uses of that information for purposes ranging from employment selection decisions to college admissions, from the likelihood of inmate recidivism to a person's social credit, and from influencing a person's consumer goods purchases to manipulating their political views, the concerns expressed by the Committee's report might offer a fair reflection on the negative impacts that have resulted from widespread data aggregation by the private sector.

III. KEY FINDINGS OF THE CHURCH COMMITTEE REPORT

Key concerns identified by the Church committee in its report included the following:

"1. The Number of People Affected…"[29] Here, the final Report pointed to the fact that at least half-a-million domestic intelligence files had been produced, including tens of thousands of detailed financial files; hundreds of thousands of pieces of mail had been read; and millions of telegrams had been intercepted.[30] Although these numbers were staggering in the 1970s, the extent to which the private sector reviews individuals' private communications puts this scale of activity to shame. Google and Facebook each review the content of many millions of emails, direct messages, and other communications every day, along with non-communications content such as the keywords used in internet searches.[31] Although lawsuits have at times been filed against these companies alleging violations of the Wiretap Act and related provisions, none thus far have succeeded.[32]

---

28. *Id*.

29. *Id.* at 5.

30. *Id.* at 290–91.

31. *See* Samuel Gibbs, *Gmail Does Scan All Emails, New Google Terms Clarify*, THE GUARDIAN (Apr. 15, 2014), theguardian.com/technology/2014/apr/15/gmail-scans-all-emails-new-google-terms-clarify ("Google's ads use information gleaned from a user's email combined with data from their Google profile as a whole, including search results, map requests and YouTube views."); *see also* Sarah Frier, *Facebook Scans The Photos and Links You Send On Messenger*, BLOOMBERG (Apr. 4, 2018, 2:06 PM), https://www.bloomberg.com/news/articles/2018-04-04/facebook-scans-what-you-send-to-other-people-on-messenger-app ("Facebook Inc. scans the links and images that people send each other on Facebook Messenger, and reads chats when they're flagged to moderators").

32. *See, e.g.*, Roxana Hegeman, *Man Sues Facebook Over Privacy Issues*, NBC NEWS (Oct. 26, 2011), http://www.nbcnews.com/id/44809232/ns/technology_and_science-security/t/man-sues-facebook-over-privacy-issues/#.XYbXaJNKh0s (reporting that a Facebook user's suit, which alleged that Facebook violated wiretap laws by tracking the user's browsing data outside of the app, will likely fail, because plaintiffs who litigate similar matters are typically unable to show harm).

"2. Too Much Information Is Collected For Too Long."[33] Here, the report noted that "Intelligence agencies have collected vast amounts of information about the intimate details of citizens' lives and about their participation in legal and peaceful political activities.[34] The targets of intelligence activity have included political adherents of the right and the left, ranging from activist to casual supporters.[35] Investigations have been directed against proponents of racial causes and women's rights, outspoken apostles of nonviolence and racial harmony; establishment politicians; and advocates of new life styles."[36] According to the report, this data collection had persisted for decades.[37] One of the areas of private sector data privacy practices that has come under increasing scrutiny is the persistence, over time, of the detailed profiles that are created. Many companies are unable to articulate a specific age-off time for data collected about individuals. This stands in stark contrast to the "right to be forgotten" recognized by European courts with respect to information which may be fully accurate, but which has been viewed as being too old to be of continued relevance when weighed against the privacy impact to the individual of continuing to make that information available.[38]

"3(a) Covert Action and the Use of Improper Means."[39] Here, the Report noted that government agencies had used detailed personal information about individuals to discredit them, cause harm to their personal relationships and employment status, and to prompt attacks against those individuals.[40] This detailed personal information was also used to propagate misinformation in an attempt to dissuade citizens from pursuing lawful rights such as the right to assembly under the First Amendment.[41] These findings have remarkable echoes with the work of groups such as Cambridge Analytica in influencing the U.S. presidential election in 2016, an area of concern described in further detail in subsequent sections of this article.

"3(b) Illegal or Improper Means."[42] Here, the Committee's Report noted that "the surveillance which we investigated was not only vastly excessive in breadth and a basis for degrading counterintelligence actions, but was also often conducted by illegal or improper means."[43] These means included reading individuals' mail,

33. S. REP. NO 94-755, Book II, at 7.

34. *Id.* at 7–10.

35. *Id.*

36. *Id.*

37. *Id.*

38. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 99 (interpreting EU Data Protection Directive to provide data subjects with a right to be forgotten).

39. S. REP. NO 94-755, Book II, at 10–12.

40. *Id.*

41. *Id.*

42. *Id.* at 12–13

43. *Id*. at 12.

wiretapping their phones, installing microphones in their homes and offices, and encouraging citizens to serve as informants on each other.[44]

"4. Ignoring the Law."[45] This section of the Report noted that, "Officials of the intelligence agencies occasionally recognized that certain activities were illegal, but expressed concern only for "flap potential."[46] Even more disturbing was the frequent testimony that the law, and the Constitution were simply ignored."[47] Here, the phrase "intelligence agencies" could easily be substituted with "digital platform providers" and a similar attitude would emerge.[48]

"5. Deficiencies in Accountability and Control."[49] Here, the Report noted that, "The overwhelming number of excesses continuing over a prolonged period of time were due in large measure to the fact that the system of checks and balances … was seldom applied. Guidance regulation from outside. . . - where it has been imposed at all – has been vague."[50] The Report continued; "there has been, in short, a clear and sustained failure by those responsible to control the intelligence community and to ensure its accountability. There has been an equally clear and sustained failure by intelligence agencies to fully inform the proper authorities of their activities and to comply with directives from those authorities."[51] The clearest analogy is to the work of the Federal Trade Commission ("FTC") in regulating the activity of technology companies, and particular the major platform providers. Despite the fact that a number of companies are subject to existing consent decrees because of the failures in their privacy practices, the FTC often lacks the resources to carry out effective enforcement, and the companies subject to those decrees are not necessarily forthcoming in their ongoing cooperation with the FTC and other similar regulatory bodies.[52]

"6. The Adverse Impact of Improper Intelligence Activity."[53] According to the report, "many of the illegal or improper disruptive efforts directed against American citizens and domestic organizations succeeded in injuring their targets. . .

44. S. REP. NO 94-755, Book II, at 12–13.

45. *Id.* at 13

46. *Id.*

47. *Id.*

48. Facebook, for example, has been accused of misrepresenting its user privacy practices. *See* Federal Trade Commission, *infra* note 53, at 1.

49. S. REP. NO 94-755, Book II, at 14.

50. *Id*. at 14.

51. *Id.* at 15.

52. For example, Facebook was fined $5 billion by the FTC for allegedly violating a 2012 consent decree, the terms of which were intended to prohibit Facebook from making misrepresentations about user privacy, and to require them to put reasonable safeguards in place. Lesley Fair, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, Federal Trade Commission (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

53. S. REP. NO. 94-755, Book II, at 15–17.

sometimes the harm was readily apparent. . . but the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale."[54] These harms included "general efforts to discredit" individuals; "media manipulation" to shape public opinion regarding particular individuals, groups, or causes; "distorting data to influence government policy and public perception"; "chilling First Amendment rights"; and "preventing the free exchange of ideas."[55]

"7. Cost and Value."[56] Finally, the Report noted that domestic intelligence activities were expensive. In the context of this report, the Committee was looking specifically at expenditures from the public coffer.[57] Here, too, however, there is an analogy to be drawn with private sector data collection. It's axiomatic in Silicon Valley that "if you're not paying for the product, you are the product."[58] The question that members of Congress and the public are beginning to ask is: what is the cost – in terms of economic value to the consumer, lost competition, and other measures of societal and individual impact – of these data collection and use practices which, until now, have been largely viewed as "free."

Each of these key findings has parallels in the 21st century risks associated with data-driven technologies. To be sure, it remains vitally important to protect against government misuse of personal information. But these risks have now been spread in ways that mere oversight of government activity is no longer sufficient to protect against the harms to individuals that may be associated with the creation, collection, and use of personal data. As Congress continues to debate multiple approaches to a potential federal data privacy law,[59] it will be essential for Congress to consider not only the contours of any specific legislative proposal that is presented for a vote, but also the manner in which Congress will organize itself in order to be best positioned to engage in the long-term legislative and investigative work that will be necessary to protect the rights of individuals and appropriately balance those rights against other important social goods and national values as data-driven technologies continue to advance and evolve.

---

54. *Id*. at 15.

55. *Id.* at 15–17.

56. *Id.* at 18.

57. *Id.* at 18.

58. *See, e.g.*, Jonathan Zitrain, *When Something Online is Free, you're Not the Customer, you're the Product*, FUTURE OF THE INTERNET BLOG (Mar. 21, 2012), http://blogs.harvard.edu/futureoftheinternet/2012/03/21/meme-patrol-when-something-online-is-free-youre-not-the-customer-youre-the-product/; *see also* Will Oremus, *Are you Really the Product: The History of a Dangerous Idea*, SLATE (Apr. 27, 2018), https://slate.com/technology/2018/04/are-you-really-facebooks-product-the-history-of-a-dangerous-idea.html (articulating a slightly different view, and an expanded history of the phrase).

59. *See, e.g.*, Cameron F. Kerry, *Game on: What to Make of Senate Privacy Bills and Hearing*, BROOKINGS INST.: TECHTANK BLOG (Dec. 3, 2019), https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

IV. CONGRESSIONAL MECHANISMS FOR CARRYING OUT INTELLIGENCE OVERSIGHT

In 1976, the Senate passed Senate Resolution 400, a resolution "To establish a Standing Committee of the Senate on Intelligence and for other purposes."[60] The legislative history that accompanied the Senate Government Operations' Committee report on the proposal noted that carrying out effective oversight of intelligence activities had long been an intractable problem.[61] The Committee noted, perhaps with some frustration, that "since the passage of the National Security of Act of 1947, establishing the National Security council and the Central Intelligence Agency," – nearly thirty years before the drafting of this report – "Congress has tried in a number of different ways to achieve close Congressional supervision of the intelligence activities of the Government."[62] Not that the Committee was keeping score, but the next paragraph of its report noted that the first legislative proposal for Congressional oversight committees had been introduced in the House in 1948 – and that nearly 200 similar bills had been introduced between 1948 and the issuance of the Committee's report in 1976.[63] The creation of committees with specifically designated intelligence oversight functions could enhance oversight in a number of ways, including by "insur[ing] the existence of a trained, specialized, and dedicated staff to gather information and make independent checks and appraisals of [intelligence] activities . . ."[64]

The drafters of the Resolution recognized the inherently interdisciplinary nature of the work that the Committee would be asked to do, and for this reason the resolution specifically required that the Committee include bipartisan membership from already-existing committees with particularly relevant equities, jurisdiction, or expertise. Specifically, the resolution called for the Senate's Select Committee on Intelligence to include fifteen members total; including two members from the Appropriations Committee, two members from the Armed Services Committee, two members from the Foreign Relations Committee, and two members from the Judiciary Committee.[65] The members who overlapped with those other designated committees were to include one from each major party, so that there would be both a majority and minority voice representing those equities on the intelligence committee.[66] The remaining seven members of the committee were to be selected from the Senate at large.[67] The Senate drafters took pains to avoid the creation of rigid stovepipes.

60. S. RES. 400, 94th Cong. (1976) (enacted).
61. *See* S. REP. No. 94-675, 3–6 (accompanying S. Res. 400, 94th Cong. (1976)).
62. *Id.* at 3.
63. *Id.*
64. *Id.* at 5.
65. S. Res. 400, 94th Cong., § 2(a)(1) (1976) (enacted).
66. *Id.* § 2(a)(2).
67. *Id.* § 2(a)(1).

This new select committee would have the right to review legislation from any other committee insofar as it touched on the intelligence-related matters that fell with the select committee's jurisdiction. A reciprocal right was established for other committees to continue to be able to study and review any intelligence-related activity that fell within that committee's jurisdiction.[68] The Resolution granted substantive power to the Committee by conferring subpoena power on the Committee, and it avoided the trap of wholly partisan-driven work by allowing subpoenas for witnesses or documents to be issued by the Chair, who would be a member of the majority political party, or the Vice Chair, from the minority party, as well as by any other Committee member authorized by the Chair or Vice Chair.[69] The Resolution also required the new select committee on intelligence to make "regular and periodic reports" to the Senate on the nature and extent of intelligence activities to the Senate as a whole.[70]

The Church and Pike Committees were initially established by Congress as temporary mechanisms; special select committees to examine the urgent, pressing concerns facing the nation about the conduct of intelligence activities that affected U.S. persons.[71] Part of the reason why they were necessary was that, up until that time, there was no single set of committees with jurisdiction over the activities of the agencies and departmental components that had become the U.S. intelligence community. As the work of the Committees proceeded, it became evident that there would be an ongoing need for committees with the scope, resources, jurisdictions, tools, and composition necessary to examine wide-ranging activities that impacted multiple dimensions of U.S policy, including national security, defense, foreign affairs, civil rights, civil liberties, free speech and association, political expression, and more.

Congress was prompted into comprehensive oversight actions in the 1970s by the urgency, scope, and complexity of challenges raised by the ways in which the U.S. Intelligence Community was collecting and using personal information – particularly about Americans – to support wide-ranging and often murky national security and policy goals. In the half-century since then, the creation, collection, and use of personal information has become far more widespread with the consequences which touch nearly all aspects of our lives. The purposes of the collection today are equally murky. Today, however, these activities are frequently carried out by private sector entities who face far less stringent regulation than that which has been the norm for the Intelligence Community ever since Church and Pike. Congress would do well to embrace the sense of urgency that pervaded its intelligence hearings in the 1970s, and take similar steps: defining the social costs

68. *Id.* §§ 3(a)(2), 3(c).

69. *Id.* §§ 5(a)(6), 5(c).

70. *Id.* § 4(a).

71. *See supra* text accompanying notes 1–2 (discussing the establishment of the Church and Pike Committees).

associated with the use of personal data, and the gaps in existing Congressional oversight regimes, and creating a new framework for data privacy oversight that is equipped to tackle the challenge of modern data usages.

V. A NON-EXHAUSTIVE SAMPLE OF DATA-DRIVEN POLICY CONCERNS THAT CROSS COMMITTEE LINES: PRIVACY AND SO MUCH MORE

For even a casual observer of issues arising at the intersection of technology and law, it's undeniable that the rate at which technology is advancing far outpaces the speed with which the law evolves. These technologies implicate individual privacy interests, where privacy is defined according to legal standards that have evolved over the past century. What is sometimes less obvious to the public and to lawmakers is that these same data-driven technologies implicate other interests, beyond a narrowly-constrained set of rights to seclusion as in the American right to be let alone, discussed in more detail below, or right to be forgotten, as has been recognized in European jurisprudence,[72] or the right to request access to, and correction and deletion of, information about oneself as in the California Consumer Privacy Act[73] and European Union General Data Protection Regulation.[74]

The ways in which personal information about individuals can be used to drive access to rights, privileges and opportunities,[75] manipulate consumer behavior[76] and sway individual political opinion,[77] used by employers,[78] insurers,[79] adversarial foreign governments,[80] and other actors all point to the challenges of data-driven technology that extend beyond traditional notions of privacy. The discussion below provides a brief overview of the origins of the legal definition of privacy in American

72. C-131/12, Google Spain v. Agencia Esspanola de Proteccion de Datos, 2014 E.C.R 317.

73. *See* CAL. CIV. CODE §§ 1798.100, 1798.105 (2018).

74. *See* Commission Regulation 2016/679, General Data Protection Regulation, art. 15–17. (articulating the "Right to Access," "Right to Rectification," and the "Right to Erasure").

75. *See generally* Meredith Whittaker et al., *AI Now Report*, AI Now Institute (Dec. 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf. The Report specifically notes that advances in artificial intelligence have led to a number of troubling trends, including "amplifying widespread surveillance," that "governments are rapidly expanding the use of automated decision systems without adequate protections for civil rights," that there is "rampant testing of AI systems "in the wild" on human populations." *Id.* at 8.

76. *See, e.g.*, Wolfie Christl, *How Companies Use Personal Data Against People: Automated Disadvantage, Personalized Persuasion* (Working paper by CrackedLabs 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf.

77. *See, e.g.*, 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 20 (2019), https://www.justice.gov/sco.

78. *See, e.g.*, *Written Testimony of Eric M. Dunleavy, PhD, Director Personnel Selection and Litigation Support Services Group, DCI Consulting, on behalf of the Society for Human Resources*, EEOC (Oct. 13, 2016), https://www.eeoc.gov/eeoc/meetings/10-13-16/dunleavy.cfm.

79. Testimony of Stephen Simchak before the United States International Trade Commission hearing on Global Digital Trade I: Market Opportunities and Key Foreign Trade Restrictions, Inv. No. 332-561, USITC Pub. 4716.

80. *See* Mueller *supra*, note 78.

jurisprudence, as well as a non-exhaustive handful of examples of ways that data-driven technologies which rely on personal information can have impacts that fall outside the scope of "privacy" as that term is sometimes narrowly understood.

Taken together, and as will be discussed in further detail in the final section of this article, the range and diversity of these challenges underscores the reasons why new Congressional committees, specifically composed of members from other relevant committees, supported by professional staff with relevant and in some cases specialized backgrounds, are vitally important to Congress's ability to keep pace with the impact of data-driven technologies on individual liberties and on American life.

A. Defining and Legislating Privacy

The right to privacy in American jurisprudence was famously articulated by Samuel D. Warren and Louis D. Brandeis in their 1890 article, "The Right to Privacy."[81] The article, discussed in more detail below, was rooted in the very same set of tensions that arise today. The authors shared a generalized sense that there should be some recourse or remedy for intrusive actions that a civilized society would see as an affront.[82] Changes in technology had made those intrusions more frequent and more troubling and although they would argue that longstanding common law traditions supported a right to privacy, it was also the case, prior to publication of their article, that American jurisprudence had not yet provided a clear model to articulate the specific set of rights or remedies that could be brought to bear in addressing these concerns.[83]

The groundwork for Warren and Brandeis' article had been laid in the years leading up to its publication. One stone in that foundation was laid in 1880, when journalist and newspaper editor E.L. Godkin wrote about the need for a free press to investigate politicians and political candidates, and the necessary balance between that vital role in gathering and exposing information and the costs to reputation and privacy that result from it.[84] While the bulk of the article is devoted to a discussion of libel, not privacy,[85] Godkin has harsh criticism both for journalism and the law.

He noted that "some of the most prominent newspapers in the country have laid the foundation of enormous commercial success by wholesale indulgence in libel. They have found, in other words, steady and persistent attacks on the reputation of individuals to be the best mode of gaining the ear of the public and extending

81. *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

82. *Id.*

83. *Id.*

84. *See generally* E.L. Godkin, *Libel and Its Legal Remedy*, 46 ATLANTIC MONTHLY 729 (1880).

85. *Id.*

their circulation."[86] He further writes that "Anglo-Saxon law, as well as Anglo-Saxon politics, has never taken much account of sentimental grievances; that is, of injury to the feelings. It cares for property greatly, and attacks on property move an Anglo-Saxon community to any needful extreme of severity in repression. It feels the deepest sympathy with the man who loses it, but it is unwilling to concern itself much about any man's mental suffering, unless he can show that he is out of pocket by it."[87] The essence of Godkin's examples, of course, lie in personal data. Without information about a person's life, however revealing, sensitive, or intimate that information might be, newspapers would have no basis for tarnishing any individual's reputation. In words that bear striking echoes of the Church Committee's analysis of intelligence activities, Godkin writes that American jurisprudence takes the view that "the press is performing a useful public function, in which, however, it is apt to commit excesses and make slips, which have to be treated with a certain indulgence."[88] It is against this backdrop that Godkin laments the fact that 19th century American jurisprudence did so little to recognize compensable harm to a person's privacy unless those harms could be directly tied to a pecuniary loss.

In Godkin's view, a person's "private life … to every man who is worth much, make[s] up by far the better part of his whole life."[89] This "private life" consisted of "that portion of the personality which is not physical or tangible, the tastes, habits, prejudices, sensitiveness, manners, relations with friends and family, and the like, about which the civilized man ordinarily dislikes to talk to strangers or have strangers talk."[90] Godkin writes approvingly of the French legal standard under which even information which is true may be actionable, simply because "a newspaper spoke of matters in [a person's] private life."[91]

Thanks to the intrusions of a salacious and widespread press, in modern life, a person's private life is always at risk:

> We have got so far away, in our newspaper ethics, from the point of view on which this legislation rests that there are but few newspapers which do not, on the slightest pretext, publish everything they can learn of all that portion of a man's sphere to which he least like to admit the world outside; and the practice grows. There never was a time when people did not enjoy hearing about their neighbor things which they knew he would not like to tell them. But as long as our law has a policy, as long as legislation aims to favor particular manners or customs from a regard

86. *Id.* at 733.
87. *Id.*
88. *Id.* at 735.
89. *Id.* at 736.
90. E.L. Godkin, *Libel and Its Legal Remedy*, 46 ATLANTIC MONTHLY 729, 736 (1880).
91. *Id.*

> to the general good, we must admit that nothing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion.[92]

Godkin's plea for re-examination of libel laws in America was written in a tone both earnest and heartfelt, one that pointed to the important policy reasons why notions of privacy ought not be limited to contexts in which it was easy to point to a threatened property interest. "I am addressing those," he wrote, "who think that the private character and individual peace of mind are things for which a civilized community is bound to provide… the community has a good deal to fear from what may be called excessive publicity, or rather from the loss by individuals of the right of privacy."[93]

The framing of his argument made clear Godkin's view that a chief threat to privacy stemmed from advances in technology – in the form of more widespread news outlets – coupled with the growth in volume and variety of personal information that was available, in 1880, about ordinary individuals. Godkin wrote,

> When we consider the enormous increase in the number of newspapers which has taken place in the last half century, and the extent to which vast communities now rely on them for nearly all they know, or wish to know, of what goes on in the world outside private houses, one is forced to admit that to no art has the progress of invention and the growth of population made such additions as to the art of holding persons up to public odium or contempt. Down to the beginning of this century, the power of any one person over any other person's reputation or feelings, through what he might say or write about him, was very trifling. It could be exercised over only a very small area and within hearing of a very small number, and, as a matter of fact, a man could readily get rid of a damaged reputation by moving away a short distance.[94]

With the 19th century advent of daily newspapers – that is, with the technological advances of the day – it was possible for individuals to suffer not just once, but from the "aggravation which results from *repetition*."[95] It is all of these factors combined which made the 19th century press the chief enforcer of "received social morality," as, in Godkin's view, "we have come more and more to rely, for the sanction of our social morality, on the strong concentration of public

92. *Id.*
93. *Id.* at 738.
94. *Id.* at 730.
95. *Id.* at 734.

opinion"[96] – and these opinions were largely set by the papers of that day. Much as they are shaped by both press and social media today.

It was against this backdrop that Brandeis and Warren famously conceptualized the right to privacy as being encapsulated in the "right to be let alone."[97] Over time, that right to be left alone was further defined by William Prosser, in a particularly influential article, as consisting of four distinct but related causes of action: 1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs. 2) Public disclosure of embarrassing private facts about the plaintiff. 3) Publicity which places the plaintiff in a false light in the public eye. 4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[98] This four-part definition has formed the basis of much of the tort theory of privacy law.

Tort law is only the tip of the iceberg, as privacy law also stems from the Constitution, from federal and state legislation, from regulatory guidance and enforcement actions, and as American privacy law is increasingly influenced by international privacy law. Against this background, privacy scholars in recent years have pointed to the shortcomings of Prosser's four-part formulation of the Warren-Brandeis "right to be let alone." One noted scholar, Daniel Solove, has pointed to a six-part conception of privacy that intersects in important ways with this article's discussion of the ways in which the current Congress is ill-equipped to consider and address policy challenges raised by digital technologies.[99] According to Solove, privacy should be thought of broadly, and includes the following: 1) the right to be let alone, 2) the right to limit others' access to the self, 3) the right to secrecy, 4) the right to exercise control over one's personal information, 5) a right to personhood that encompasses two key formulations in the right to individuality, dignity, and autonomy and the right to anti-totalitarianism, and 6) the right to intimacy.[100] With this broader conceptualization of privacy, a great deal more could be encompassed than is currently the case under traditional notions of privacy torts.

The challenge in defining "privacy" is evident in current Congressional hearings on federal privacy legislation. Ever since the adoption by the Department of Health, Education, and Welfare of the Fair Information Privacy Practices ("FIPPs")[101] in the 1970s, the U.S. approach to privacy, from both a legislative and executive standpoint, has been a largely sectoral one. Contrary to the frequent, and

96. E.L. Godkin, *Libel and Its Legal Remedy*, 46 ATLANTIC MONTHLY 729, 729 (1880).

97. Warren & Brandeis, *supra* note 82, at 193.

98. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

99. *See generally,* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

100. *Id.* at 1099–25.

101. U.S. DEPT. OF HEALTH, EDUC., AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

somewhat self-serving, criticism levied by the nations of the European Union,[102] the sectoral approach has not left U.S. privacy law toothless or ineffectual. However, it has led to a segmented approach to privacy legislation.

For example, Health care privacy is regulated by the Health Insurance Portability and Availability Act ("HIPAA") and its amending legislation, the Hi-TECH Act.[103] Genetic information is regulated – for limited purposes related to employment and insurance only – by the Genetic Information Act ("GINA").[104] Financial information is regulated within financial services industry by the Graham-Leach-Bliley Act ("GLBA").[105] Children's online information is regulated by the Children's Online Privacy Protection Act ("COPPA").[106] At the state level, all fifty states, as well as the District of Columbia, Puerto Rico, and Guam, have data breach legislation that applies to personal information.[107] Although each of these states has defined its own scope and applicability, the current laws[108] generally share similar attributes, serving as consumer protection statutes that require notification to individuals if there is a breach of information such as Social Security numbers, payment card

102. *See, e.g.*, Jennifer Strong, *Where European Countries Stand on Privacy vs. Security*, PUBLIC RADIO INT'L. (Mar. 11, 2016, 8:15 AM), https://www.pri.org/stories/2016-03-10/where-european-countries-stand-privacy-versus-security.

103. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); 45 C.F.R. §§ 160, 164 (2002); Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5 § 3001, 123 Stat. 115, 226-32 (2009).

104. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233 § 105, 122 Stat. 881 (2008).

105. Gramm-Leach-Bliley Act, Pub. L. 106–102, 113 Stat. 1338 (1999).

106. Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506 (1998).

107. *Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

108. The California Consumer Privacy Act (CCPA) provides a notable exception to the overall similarity of state data breach laws. *See generally* Cal. Civ. Code §§ 1798.100-.199 (Deering 2018). The CCPA was passed in 2018 with an effective date of 2020, and established a number of new data privacy rights for consumers and data privacy obligations for certain collectors and processors of personal data. The CCPA has been compared to the European Union's General Data Privacy Regulation (GDPR), with a number of commentators pointing to aspects of the law which are more analogous to the GDPR than to traditional data breach laws in U.S. states. Throughout 2019, there were a number of hearings held by the California Attorney General addressing concerns about the legislation, including the need for additional clarity and precision with respect to some definitions in the law. The California General Assembly passed a number of amendments which were signed into law by the Governor of California in October 2019. *See, e.g.,* Assemb. B. 1355, 2019-20 Leg., Reg. Sess. (Cal. 2019) (amending to exclude consumer information that is deidentified or aggregate consumer information from the definition of personal information). As of this writing, the California Attorney General has issued draft regulations and is reviewing public comments; final regulations have not yet been promulgated. As a result, some aspects of the law's implementation and effect remain unresolved.

information, and in some statues, passwords for electronic accounts, biometrics, and health or other sensitive data.[109]

When we look just at the privacy dimensions of the policy questions raised by data-driven technologies, no single committee has sufficiently comprehensive jurisdiction to tackle all the issues that need to be considered with respect to particular technologies. For example, in just one week in May, 2019, privacy-related hearings were held in four separate Congressional committees.[110] The Senate Commerce Committee held a hearing titled, "Consumer Perspectives: Policy Principles for a Federal Data Privacy Framework."[111] Less than a week later, the Senate Appropriations Committee's Subcommittee on Financial Services and General Government held a hearing addressing the budget for the Federal Trade Commission, the nation's top consumer protection watchdog and the agency which has taken the lead on most consumer privacy regulation and enforcement actions.[112] The Senate Banking Committee held a hearing titled "Privacy Rights and Data Collection in a Digital Economy."[113] Finally, the House Energy and Commerce Committee held an oversight hearing on activities of the Federal Trade Commission to strengthen data privacy and security protections.[114] Congressional focus on privacy legislation has continued throughout 2019, with further hearings,[115]

109. *2019 Security Breach Legislation*, NATIONAL CONFERENCE OF STATE LEGISLATURES (July 26, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx#2019.

110. *See Congress Continues Hearing into Federal Privacy Legislation,* NEWS MEDIA ALLIANCE (May 8, 2019), https://www.newsmediaalliance.org/congress-continues-hearings-into-federal-privacy-legislation/.

111. *Consumer Perspective: Policy Principles for a Federal Data Privacy Framework,* U.S. SENATE COMMITTEE ON COM., SCI & TRANSP. (May 1, 2019, 10:00 AM), https://www.commerce.senate.gov/2019/5/consumer-perspectives-policy-principles-for-a-federal-data-privacy-framework.

112. *Review of the FY202 Budget Request for the FCC & FTC,* U.S. SENATE COMMITTEE ON APPROPRIATIONS (May 7, 2019, 2:30 PM), https://www.appropriations.senate.gov/hearings/review-of-the-fy2020-budget-request-for-the-fcc-and-ftc.

113. "Privacy Rights and Data Collection in a Digital Economy," Hearing, May 7, 2019, https://www.banking.senate.gov/hearings/privacy-rights-and-data-collection-in-a-digital-economy

114. *Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for American's Privacy and Data Security*, HOUSE COMM. ON ENERGY & COMMERCE (May 8, 2019), https://energycommerce.house.gov/committee-activity/hearings/hearing-on-oversight-of-the-federal-trade-commission-strengthening.

115. *See, e.g.*, *Examining Legislative Proposals to Protect Consumer Data Privacy*, U.S. S. COMM. ON COMMERCE, SCIENCE, & TRANSPORTATION (Dec. 4, 2019), https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy.

multiple bills introduced in Congress,[116] and a group of Senate Democrats issuing a statement of principles that they view as necessary to any federal privacy law.[117]

There is a long list of primary committees within Congress that have jurisdiction over some aspect of the impacts of data-driven technologies. On the Senate side, these include the Commerce, Science & Transportation Committee,[118] the Homeland Security and Government Affairs Committee,[119] the Select Committee on Intelligence,[120] and the Judiciary Committee.[121]

On the House side, these include the Energy and Commerce Committee,[122] the Homeland Security Committee,[123] the House Permanent Select Committee on Intelligence,[124] the Judiciary Committee,[125] the Space, Science, and Technology Committee.[126] In addition to these nine primary committees, a handful of additional committees – such as the Senate Banking Committee – have subcommittees that can lay claim to jurisdiction over at least some sliver of data privacy, data-driven discrimination, government surveillance, and data-driven technologies as a key economic and trade engine for the U.S.[127]

---

116. *See, e.g.*, *Cantwell, Senate Democrats Unveil Strong Online Privacy Rights*, https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights. Reports in early December of 2019 that Republican Senator Roger Wicker had circulated a draft consumer privacy bill that, as of this writing, was not yet formally introduced. David Shepardson & Diane Bartz, *Republican Privacy Bill would set U.S. Rules, pre-empt California: Senator*, REUTERS (Dec. 2, 2019), https://www.reuters.com/article/us-usa-privacy-congress/republican-privacy-bill-would-set-us-rules-pre-empt-california-senator-idUSKBN1Y62EO.

117. *Privacy and Data Protection Framework*, https://www.democrats.senate.gov/imo/media/doc/Final_CMTE%20Privacy%20Principles_11.14.19.pdf.

118. S. Doc. No. 113-18, at 21 (2013) (dealing with issues ranging from communications, highways, aviation, rail, shipping, transportation security, merchant marine, the Coast Guard, oceans, fisheries, weather, disasters science, space, interstate commerce, tourism, consumer issues, economic development, technology, competitiveness, product safety, and insurance).

119. S. Doc. No. 113-18, at 24 (2013) (overseeing Department Homeland Security).

120. H.R. Res. 658, 95th Cong. (1977) (authorizing the Select Committee on Intelligence to oversee and make continuing studies of the intelligence activities and programs of the United States Government).

121. S. Doc. No. 113-18, at 25 (2013) (providing oversight of the Department of Justice and the agencies under the Department's jurisdiction, including the Federal Bureau of Investigation, and the Department of Homeland Security).

122. *Jurisdiction*, HOUSE COMM. ON ENERGY & COMMERCE, https://energycommerce.house.gov/about-ec/jurisdiction.

123. *Privacy, Civil Rights, & Civil Liberties*, COMM. ON HOMELAND SECURITY, https://homeland.house.gov/issues/privacy-civil-rights-civil-liberties.

124. *Rules of Procedure for House Permanent Select Committee on Intelligence 116th Congress*, https://docs.house.gov/meetings/IG/IG00/CPRT-116-HPRT-IG00-CommitteeRules.pdf.

125. U.S. HOUSE COMM. ON THE JUDICIARY, https://judiciary.house.gov/issues.

126. *History and Jurisdiction*, U.S. HOUSE OF REPRESENTATIVES COMM. ON SCIENCE, SPACE, & TECH. (last visited Oct. 18, 2019), https://science.house.gov/about/history-and-jurisdiction.

127. *Jurisdiction*, UNITED STATES COMM. ON BANKING, HOUS., AND URBAN AFFAIRS (last visited Dec. 20, 2019), https://www.banking.senate.gov/about/jurisdiction.

In some instances, the decision about which committees have jurisdiction over particular topics has been driven by the way in which subject matter is defined – for example, as consumer privacy, health privacy, government surveillance, children's online privacy. In other instances, overlaps and duplications of committee jurisdiction, or gaps between committee jurisdiction, have been driven by the ways in which regulatory responsibility is apportioned across federal agencies. For example, committees with oversight authority over the Federal Trade Commission may hold hearings or propose legislation relating to the antitrust and consumer protection implications of data-driven technologies. In still other instances, committee jurisdictions are tied to the underlying legal authority – such as the First or Fourth Amendments to the Constitution. In each of these cases, however, overlaps exist.

Imagine, for example, a mobile app that collects individual health data and shares that data with social media platforms, insurance companies, companies that perform background checks for employment, data brokers, and political campaigns. On the Senate side, the collection and use of that data could be addressed by hearings in the Senate Health, Education, Labor and Pensions Committee (addressing health privacy and the use of health data in employment); the Senate Commerce Committee (focused on consumer protection and antitrust); the Senate Banking Committee (examining whether use of health data in employment-related background checks is consistent with the Fair Credit Reporting Act); the Senate Homeland Security Committee (examining election security and whether voters' individual health care data was being accessed and used by foreign powers to manipulate voter opinion in elections where health care policy was a campaign issue), the Senate Judiciary Committee (addressing the use of digital advertising in election manipulation), and so on. An equally complex picture of possible oversight hearings would emerge on the House side.

Overlapping jurisdiction among committees is not new in Congress, nor does it need to be abolished. Where, however, multiple committees focus on only a subset of the issues relating to a single set of facts, that narrow focus raises a real risk that gaps will arise. If the hypothetical scenario above prompted widespread public concern, it's likely that all of these committees – and perhaps more – would hold hearings and consider whether legislation is needed to restrict how this data is collected, combined, or used. If, on the other hand, the scenario prompted only low-level, routine concern among one of the many committees with jurisdiction over a part of this pattern of facts, then it is entirely possible that Congressional review could investigate some questions and altogether overlook other, equally important, ones.

B. Data-driven Impacts that Extend Beyond "Privacy": A Non-Exhaustive Sample of Illustrative Examples

Data-driven technologies have impacts that intersect with, and range far beyond, privacy. These impacts include pressing challenges and include the potential for racially and ethnically discriminatory outcomes from artificial intelligence and machine learning algorithms. The use of personal data as a means for micro-targeting for commercial advertising purposes, and the use of detailed individual consumer profiles in order to manipulate elections through the development and placement of individually-targeted messages, have already been employed to exacerbate existing societal and political tensions.[128] Whether carried out by nation-states or by domestic political campaigns, the use of detailed individual profiles to deliver surgically targeted political advertising, which addresses not just high-level demographics such as age, gender, zip code and income, but also features such as personality profiles, in order to sway elections raises a host of privacy-adjacent considerations that were not nearly as pressing in the context of older, analog-era direct marketing campaigns.

If these other impacts were entirely independent of privacy concerns, then perhaps each of these could be sensibly addressed in isolation from each other, each in its own stovepipe, each falling within the jurisdiction of a specific, discrete committee. Nothing, however, could be further from the truth. Privacy implications are intertwined with each of these other impacts, because all of these impacts arise from the use of granular personal information by data-driven technologies that can be employed by multiple actors for multiple purposes and with multiple outcomes. Consequently, none of these data uses or issues can be effectively addressed in a vacuum, independently of each other.

Privacy laws that aim to deal with the challenges of data-intensive technologies will be deficient if they don't also address other dimensions of rights, autonomy, personhood, and social good that are impacted by these technologies. The reverse is equally true. Any attempt to address these other impacts – including but not limited to labor laws, research standards, antitrust laws, consumer protection, political interference, election security, discriminatory policing and criminal justice impacts, First Amendment protections, international commerce, and international human rights – will also fail if they are addressed in a vacuum without consideration for more traditional privacy formulations, and without consideration for each of the other bundles of rights. As long as legislators examine laws relating to data-driven technologies in stovepiped committees with specific areas of focus, the separation of issues that is reinforced by distinct committee jurisdictional lines will exacerbate the already-difficult task of developing and passing sensible legislation to address data-driven technologies.

---

128. *See* 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 20 (2019), https://www.justice.gov/sco.

Before proposing an alternative approach structure for legislative consideration that could help close some of these gaps and move policymakers towards a more comprehensive approach to considering the challenges associated with modern data-driven technologies, it is useful to look at a handful of the disparate risks that are made possible by today's data-rich environment. The set of risks outlined below is by no means complete, nor should the order in which they appear be viewed as an attempt to rank them in any particular order of importance. Rather, the list below is a non-exhaustive catalogue of the ways in which personal data – information from individuals, about individuals, describing the features and activities of individuals – can be collected, analyzed, and used in ways that threaten harm to individual freedoms.

In other words, if what we mean by privacy is the right to screen our private life from public view, or the right to maintain certain information about ourselves in confidence, then it isn't just privacy that's at stake when information can be gathered and used in an ever-more-sophisticated number of ways. As these examples show, the personal data that is collected about us is also used to make judgments about us, and to sway our own judgments about people, products, and issues to the benefit of someone else. On the other hand, if we look at privacy in terms of the Warren-Brandeis formulation of the "right to be let alone" and construe those words to have their broad and commonplace meaning, then indeed the use of these technologies is all about "privacy." For it is through collection and analysis of this detailed information about ourselves, our personalities, our predilections and our peccadilloes, that the information can be exploited in a myriad of ways for our loss and others' gain.

C. Digital Piecework, the Survey Economy, and Unrestricted Human Subjects Research

Artificial intelligence, machine learning, and complex algorithms are in the process of transforming the global approach to a wide range of economic activities. Many of those technology capabilities require vast quantities of data to train the algorithms as well as to produce meaningful results.[129] A great deal has been written already about the challenges of the "black box" of machine learning algorithms. Black Box computer programs are self-teaching and, therefore, reach conclusions for reasons and in ways that their own programmers cannot fully predict, articulate, or explain.[130] A great deal has also been written about the ways in which implicit bias is often incorporated into these algorithms, leading to a host of impacts that have deeply negative effects on society and on individuals, from

129. *See, e.g.*, *New Technique Cuts AI Training Time by More than 60 Percent*, SCIENCE DAILY (Apr. 8, 2019), https://www.sciencedaily.com/releases/2019/04/190408114322.htm.

130. *The Dawn of Artificial Intelligence: Hearing Before S. Comm. on Commerce, Sci. & Transp.,* 114th Cong. 16 (2016) (statement of Eric Horvitz, Technical Fellow and Director, Microsoft Research, Interim Co-Chair, Partnership on Artificial Intelligence).

failing to accurately predict, identify, or assess individuals based on their gender or ethnicity,[131] to perpetuating racial bias and other forms of discrimination.[132]

In addition to these well-documented and important concerns, the rise of machine learning technology has also led to a number of unanticipated impacts relating to employment and human subjects research. Both topics that fall outside the scope of what is typically thought of as "privacy" or "privacy law" – but both of which have impacts on individuals' autonomy as well as an economic impact on society. All of which are made possible by the modern technological capacity to collect, process, and analyze cast quantities of personal data.

For example, the CAPTCHA boxes that visitors to many websites are forced to fill out, sometimes merely checking a box, and other times being asked to identify photo with particular characteristics or identify particularly hard-to-read text, are not only a means of ensuring site security by testing the likelihood that a site visitor is human.[133] These CAPTCHA boxes also monetize the site visitor's digital labor. Users' clicks are being used to train an algorithm to recognize the storefronts, crosswalks, or cars depicted in the photographs.

In doing so, the big data companies – Google in particular, which now owns CAPTCHA – are able to leverage the free labor of billions of global users. The data collected by those who have to pass CAPTCHA security gates is used to train tag and catalogue Google's data set. Google gets the labor for free, and the impact on individual is, practically speaking, so de minimis for each instance, that while people find it annoying, they are unlikely to refuse to complete a CAPTCHA request if refusing to do so would prevent them from navigating to their intended destination website.

The digital economy takes this monetization of online labor even further in the context of the survey economy, in which users are enticed to offer up detailed personal information in exchange for vanishingly small amounts of cash or other compensation. More than anything else, it's the new shape of what used to be home-based sweatshop labor. This is the 21st century digital manifestation of 19th century piecework, when poor women living in urban settings eked out a living

131. *See, e.g.*, Meredith Whittaker et al., AI Now Report 2018, AI NOW INSTITUTE, at 15 (Dec. 2018), https://ainowinstitute.org/AI_Now_2018_Report.pdf (discussing a facial recognition software study showing that Amazon's Rekognition software incorrectly identified 28 members of Congress, with a 40% error rate in non-white members of Congress, and only a 5% error rate in white members of Congress).

132. In cities such as Orlando and Washington County, Sheriff's departments have utilized Amazon's Rekognition system to detect faces and compare them against mugshots. *Id.* at 15–16. This process, however, creates cause for concern since studies have shown that facial recognition technology is better at detecting people with lighter skin tones than people with darker skin tones, and better at detecting men than women. *Id.*

133. CAPTCHA tests do this by asking users to perform tasks that people are good at – such as deciphering grainy text or interpreting poor-quality images – and that are particularly challenging for computers. A user who can successfully complete these tasks is likely a person, not a bot.

sewing shirts for pennies apiece. As the gig economy demonstrates, piecework has never really stopped.

This new incarnation in the modern economy displays all the same characteristics of class division and exploitation, with wealthy people and companies relying on those who are already poor to do the most poorly paid work. According to the Smithsonian Museum of American History, there were stark class divisions between dressmakers, who created entire garments and could earn a decent living, and impoverished seamstresses who stitched together pre-cut bundles of fabric for desperately low pay.[134] They were paid by the piece for the number of items they sewed, and often worked sixteen hours a day, but despite the long hours, earned only enough money to barely subsist. Even worse, the shop owners who assigned them the piecework often found fault with the workmanship and refused to pay the seamstresses.[135]

One of the striking facets of the sweatshop clothing industry is just how many layers of exploitation were involved. Tailors began making ready-to-wear clothes for a class of people who couldn't afford individually-tailored clothes.[136] In order to keep profit margins high, they cut the cloth themselves and turned over the pieces to slop-shop workers, usually unmarried girls and women – either young, or widowed, or otherwise in distressed circumstances. These individuals carried out the backbreaking work of assembling the pieces while hunched over in candlelight squinting at the tiny eye of each needle they had to thread and each knot that needed to be tied.[137] The tailors gravitated towards this model of work specifically for its economics; in other words, they could pay the women substantially less than they paid men. [138]

The exploitation didn't stop there. As the women's underpaid labor made it possible to produce ready-to-wear clothes for cheaper and cheaper costs,[139] these slop shop jobs began to be used to mass-produce clothing for slaves in the southern states.[140] Slaves could not be expected to purchase their own clothing, as they didn't have wages with which to buy them, and slave owners wanted to keep their

134. *History of Sweatshops: 1820-1880*, NAT'L. MUSEUM OF AM. HIST. (last visited Dec. 21, 2019), https://americanhistory.si.edu/sweatshops/history-1820-1880.

135. *Id.*

136. *Id.*

137. *Id.*

138. Ariane Hegewisch & Heidi Hartmann, *The Gender Wage Gap: 2018 Earnings Differences by Race and Ethnicity*, INST. FOR WOMEN'S POL'Y RESEARCH (Mar. 7, 2009), https://iwpr.org/publications/gender-wage-gap-2018/. The discount for female labor, of 20% to 25% percent off wages paid to men, remained almost exactly the same from the 1800s through the early 21st century. *Id.*

139. *See generally* Beth Harris, *"Slaves of the Needle:" The Seamstress in the 1840s*, THE VICTORIAN WEB (Dec. 10, 2014), http://www.victorianweb.org/gender/ugoretz1.html; Vic, *The Dress Maker and the Seamstress in Regency England*, JANE AUSTEN'S WORLD (Aug. 8, 2010), https://janeaustensworld.wordpress.com/2010/08/08/the-dress-maker-and-the-seamstress-in-regency-england/.

140. *Id.*

costs as low as possible, purchasing the least expensive supplies possible to keep their slaves able to work. Owners of capital commanded the resources to possess humans as property and to extract poverty-level wages from another class of persons. The cycle of exploitation flowed from one underclass group to another, with the wealthy slaveowners and well-to-do tailors profiting from both.

As technology advanced with the advent of the sewing machine, productivity leaped ahead. And yet, the workers didn't see more income; instead, they were offered the chance to obligate money they did not have to purchase on an installment plan the very technology that would keep them toiling away for substandard wages.[141] Concerned that the machines would put seamstresses out of work, several reformers urged manufacturers not to use them.[142] It soon became clear, however, that the rapidly expanding industry still required the labor of tens of thousands of workers. Although the machines dramatically enhanced productivity and lowered the price of clothing, they did not greatly increase the earnings of these women.[143]

The example of 19th century piecework bears striking parallels to the ways in which 21st century technology – particularly smart phones – provide a false promise of independence to modern gig workers in the data-driven economy. As explained below, however, the mismatch between promise and reality may be even greater. Where sewing machines promised independence and delivered debt, smart phones offer the allure of independent contractor status in a side hustle gig economy, while delivering low pay and long hours. In addition, a sacrifice that 19th century workers did not experienced has become commonplace: the phones that we use to perform modern sweatshop labor are also siphoning off vast quantities of detailed information about who we are, what we like, who we spend time with, and what we do.

It's as if the 19th century sewing machine not only became the instrument of a pieceworker's servitude to a vicious cycle of debt, but also served as the instrument to tell the sewing machine companies exactly how far into debt the pieceworker would go to purchase this symbol of hope. This was in addition to simultaneously serving as the vehicle for informing the tailors precisely how desperate the pieceworker was for money while also informing the company precisely how little she could be made to accept in exchange for her hours of work. As smart phones have become indispensable to everyday life, their prices have risen near towards the thousand-dollar range, and often are paid on multi-year installment plans. If social media is the opiate of the masses, then our smartphones can dull the pain of an economic existence in which they are both the offerors of our moments of perceived freedom, and the means of our enslavement. Offering us the ability to

141. *Id.*

142. *Id.*

143. *Sweatshops in America: History of Sweatshops*, NAT. MUSEUM AM. HIST., https://americanhistory.si.edu/sweatshops/history-1820-1880 (last visited Sept. 13, 2019, 12:51 PM).

have a side hustle driving for Uber or Lyft on the gig economy, delivering food for GrubHub or StreetEats, and taking surveys for money at a rate of 25 cents to a dollar an hour.

It may seem like a stretch to compare this state of affairs to the digital piecework of today's freelance survey economy, but a closer look at the business model for sites like SurveyJunkie, make it clear that the comparisons are apt. The Survey Junkie website invites readers in with an enticing call to shape consumer society: "take surveys. Get PAID. Be an influencer. Share your opinion to help brands deliver better products & services."[144] Further down the page, it says, "Make a difference as a consumer. Your opinion can change the products of tomorrow, today."[145]

The website's "testimonials" are frothy and appealing, consisting of quotes from what purport to be real people, all of whom rave about the reasons they love taking online surveys on the site. According to one, "Survey Junkie provides an interesting way to make a little cash while doing something interesting."[146] A second endorser gushes that, "I really feel like my opinion matters and I love taking the surveys. . . It's a privilege to be part of the Survey Junkie family!"[147] A third notes that, "It took some honest hard work, but I had fun doing it."[148] Another endorser on the Survey Junkie website offers the practical recommendation that, of all the online survey sites, Survey Junkie has "the best rewards."[149]

It is not just Survey Junkie. The homepage for Vindale Research tries to draw in new users with a similar pitch: "Join the finest minds in consumer research and help change the world! Share your unique opinion and get paid for it!"[150] LifePoints survey company makes a similar pitch: "Connect with the LifePoints community. Become a member of our global community while interacting with millions of other people who share their opinions. Join and be part of something special that will allow you to change your world. LifePoints is the place to be for those who want to be heard. We're the bridge that connects people's habits and views with what companies offer to consumers."[151] Global Test Market tries to entice users with the pitch that they can, "earn rewards for taking paid surveys; surveys are a fun way to learn something new; FREE to join."[152]

The marketing is deliberate. "Influencers" in the social media world are those Instagram-famous celebrities who are often famous for nothing more than being

144. SURVEY JUNKIE, https://www.surveyjunkie.com/ (last visited Sept. 15, 2019).
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. VINDALE RESEARCH, https://www.vindale.com/v/join/join4a.jsp (last visited Sept. 15, 2019).
151. LIFEPOINTS, https://lifepointspanel.com/ (last visited Sept. 15, 2019).
152. GLOBAL TEST MARKET, https://www.globaltestmarket.com/?lang=E (last visited Sept. 15, 2019).

famous. They have hundreds of thousands or millions of followers on social media – so many that every tweet and post gets thousands of likes, retweets, reposts, reshares. A single video from a YouTube influencer can shape a person's ideology. A single post on Instagram can cause sales of a beauty product to soar. No one in today's social media environment seriously believes that someone getting paid pennies for completing online surveys truly is an "influencer." But the very name appeals to our sense of existence. It gives us hope that we have some relevancy in the massively networked digital world where it's so easy to lose our true selves amidst the forest of idealized posts from friends, strangers, and influencers about all of the ways that they're crushing it in life.

By and large, however, the people filling out Survey Junkie's online surveys *are not* leading fulfilling, picture worthy lives. Many of them are college students trying to make side income to help pay for groceries in an economy in which 40% of college students experience food insecurity.[153] Others are working class and working poor – people with enough income to have a smartphone and internet access, but who are living in tight enough financial conditions that making a little bit of extra cash, any extra cash, is worth doing if there's a way to do it.

So how much money do these digital piece workers make, and what exactly do they give up in return? As part of the digital ecosystem, the world wide web abounds with sites that promise life hacks, side hustles, and ways to scrape together crumbs of cash in between more traditional hourly or salaried jobs. Bloggers know that referral links can earn them endorsements and cash, so there's some incentive to paint a rosy picture of other websites that are potential sources of endorsements. Nonetheless, a wide range of review websites paint a picture of Survey Junkie that helps advise those who haven't set up a log in yet what the experience is really like.

According to one website that provides tips on how to save money and earn extra cash in the gig economy, Survey Junkie's payment formula is pretty typical of online survey websites and may even pay better than most. Take this example: the website "clubthrifty.com" has a very positive review of Survey Junkie that opens with an enticing offer,

> Have you ever spent a lazy day around the house wishing you could make money while you relax? Well, as it turns out, there are plenty of fun ways to earn extra money for very little effort. That's right, you can hop online

153. Kaya Laterman, *Tuition or Dinner? Nearly Half of College Students Surveyed in a New Report are Going Hungry*, N.Y. TIMES (May 2, 2019), https://www.nytimes.com/2019/05/02/nyregion/hunger-college-food-insecurity.html.

> when you're not busy, and start earning right away with Survey Junkie![154]

Alert readers of the website might notice that above that beguiling intro is a text box noting that, "this article may contain references to some of our advertising partners. Should you click on these links, we may be compensated."[155] Of course, one of the clickable links is to Survey Junkie. According to this particular review, when it comes to anticipating how much money you can make, "of course, it's important to temper your expectations. The money you make won't enable an early retirement by any means, but it can pad your vacation fund, help you save for holiday gifts, or even help pay off a loan a bit faster. Even if you only spend a few hours a month taking surveys, you'll earn a few bucks you didn't have before."[156] The review emphasizes that Survey Junkie – with three million users – is "legit."[157]

There are a number of caveats to these representations. First, nearly all of the surveys require the user to answer demographic questions at the beginning of the survey. Sometimes the questionnaires are short and straightforward. Other times, simply getting through the demographics can take twenty minutes or more. The demographics are essential to advertisers who want to obtain valid survey results and require some degree of confidence that the person answering the question isn't submitting outrageous answers just for the purpose of skewing the results. Therefore, if a user's demographic answers disqualify him or her from continuing with the survey, they don't get paid at all by many survey websites.

Additionally, the best-paying surveys are ones that require the user to activate their camera and allow the survey website to capture photos and/or video of the survey-taker. Users are far more averse to this type of intrusion. However, on many websites, allowing the site to take photos or videos of the survey-taker is the price for participating in better-paying surveys.

According to one website that posts tips on saving and earning money, Survey Junkie is one of the better online survey websites.[158] Users earn twenty-five points for signing up, and additional points for every survey they complete.[159] Signing up is free and users create a login and provide Survey Junkie with demographic information that helps Survey Junkie match the user with surveys – generally sponsored by advertisers – that they fit the desired demographic mold for.[160] As

154. Kate Underwood, *Survey Junkie Review 2019: Is it a Scam or Legit?*, CLUB THRIFTY (May 16, 2019), https://clubthrifty.com/survey-junkie-review/.

155. *Id.*

156. *Id.*

157. *Id.*

158. *Id.*

159. Kate Underwood, *Survey Junkie Review 2019: Is it a Scam or Legit?*, CLUB THRIFTY (May 16, 2019), https://clubthrifty.com/survey-junkie-review/.

160. *Id.*

each potential survey is offered, the user is shown a summary. These summaries include the amount of points they can earn for successfully completing the survey, i.e., not getting disqualified in the demographic process or quitting before they survey is complete, and how many minutes they can expect the survey to take. Surveys paid as much as forty points for five minutes, or as little as forty points for twenty minutes.[161] Every time a user completed a "profile survey" – providing more information about themselves – they received another ten points.[162]

Eventually, the points are redeemable as gift cards or cash. It takes a while, though. The conversion is one dollar for every 100 points.[163] So that survey that lets the user earn forty points in twenty minutes? A user who completed three of those would earn credits at the rate of $1.20 per hour. Even worse, nothing is redeemable until the user hits $10.00 worth of points[164] – and some websites don't allow users to redeem their points for cash until they've accumulated a minimum of $20 or $25 – something that could take literally days of answering online questions.

Even the "really good" surveys that pay 10 points for a questionnaire that's estimated to take one minute to complete aren't a great deal. If a user completed sixty of those surveys, earning ten points per minute for an entire hour, continuously and with absolutely no time required to navigate from the completion of one "lucrative" survey to another, the user would still only earn a maximum of $6 worth of points, for an entire hour's work.[165] That's less than the federal minimum wage.[166] And when you consider that the user is being paid less than minimum wage *and* giving up detailed information about themselves for the privilege of doing it, it doesn't seem like such a great side hustle after all.

As it happens, the ideal of even $6 per hour is unlikely to happen in a short time, as sites like Survey Junkie often don't have enough surveys available to take. According to one reviewer, about the best a person is likely to experience is somewhere from one to three surveys per week, averaging about $12 per week.[167] All that said, a number of reviews have consistently ranked Survey Junkie as one of the best sites for this kind of online piecework, data-for-cash earning.[168] Other sites don't allow PayPal cash-outs, only gift cards or redemption by check sent through

161. *Id.*

162. *Id.*

163. *Id.*

164. *Id.*

165. Jim Wang, *A Detailed Review of My Survey Junkie Experience (2019)*, WALLET HACKS, (Feb. 26, 2019), https://wallethacks.com/survey-junkie-review/.

166. As of this writing, the federal minimum wage was $7.25 per hour. U.S. DEPT. OF LABOR, https://www.dol.gov/general/topic/wages/minimumwage.

167. Jeff Rose, *Survey Junkie Review*, GOOD FINANCIAL CENTS, (Aug. 7, 2019), https://www.goodfinancialcents.com/survey-junkie-review.

168. Jeff Rose, *13 Best Online Survey and Research Sites for Money and Rewards*, GOOD FIN. CENTS, (Sept. 9, 2019), https://www.goodfinancialcents.com/best-online-survey-sites-for-money/.

the mail. Many of them have expiration dates on points, requiring users to continue actively engaging with the site and providing more information and answering more surveys in order to get paid for the work they have already done.

All of the sites serve up questionnaires that the user is not actually eligible for – meaning that users spend time answering preliminary questions, only to get kicked out of the survey before its completed. Users find themselves ineligible for cash, points, or any other kind of payout. The older, more established survey companies often pay even less to participants. The LifePoints online survey platform grew out of a marketing research company that started conducting consumer polls in 1946.[169] Apparently, they still pay at 1946 scales, as participants can expect to earn between $.50 and $1.25 per completed survey.[170] And even Global Test Market, which has been accredited by the Better Business Bureau, only pays between $1.50 and $1.75 per completed survey.[171]

These sites all have a number of features in common. They entice users by touting the advantages of free enrollment – an advertising mechanism that's long been known to channel consumer thinking into a narrow focus on only one dimension of a multi-faceted decision.[172] They offer consumers the opportunity to feel as though they are part of something larger than themselves – as though through these surveys, they can have a direct and personal role in shaping the direction of future products, advertisements, movies, television shows, and the like. Many of them emphasize a sense of community even though interaction with other users isn't part of the online survey experience. And they all are heavily promoted on the hundreds of websites that hold themselves out as offering money-making ideas to people who are "frugal," "cash-strapped," "savvy," looking for "life hacks," or other catch phrases that can be used to appeal to a person's idea of themselves, and through that appeal, talk them into spending time giving up detailed personal data for almost no monetary return, and without the kinds of entertainment value that they receive from online social media platforms.

Looked at in this light, the survey economy has close parallels to the piecework economy of previous centuries, with the additional twist that the piece workers are enticed with inflated promises about payment and encouraged to overlook the fact that they're being paid less than minimum wage and sacrificing an enormous amount of personal information along with their time.

169. *Id.*

170. *Id.*

171. *Id.*

172. Users focus on the free enrollment and forget questions such as: How much does it pay? How much of my time will be required? How much personal data do I have to give up? What will the site do with my data? Who else will my data be shared with? Could I more profitably spend the same time doing something else?

VI. AUTOMATION OF THE TURING TEST, AND MONETIZING OUR LABOR ONLINE

If you've spent any time on the internet, you've undoubtedly navigated to a site – perhaps an online ticket broker, or a user forum – that demanded that you click on a box saying "I am not a robot" before allowing you to proceed. The site might have required you to decipher distorted text and type the letters into a box. Or perhaps you've grown increasingly annoyed by the security tests that present a grid of blurry, distorted images and require you to click on all of the storefronts, or all of the cars, or all of the pictures containing a sign, before allowing you to proceed to the website you're trying to reach.

All of these are part of a system of digital testing designed to prove whether a human or an automated software bot script – a bot – is requesting approval to navigate to the link. Over the past ten years, the most widely used method for that testing was purchased by Google.[173] Since the purchase Google uses the answers it collects, from people who have no choice but to complete the forms to surf the internet, to train Google's AI.[174] Not only is our labor in training Google's artificial intelligence unpaid; it also captures systematic information about the kinds of tasks humans can perform consistently well, and the tasks that humans have trouble with. In other words, a cynic might note that Google is using these anti-bot tests to carry out a massive, undisclosed, and uncontrolled study of human cognition, using nonconsenting data subjects who don't realize their personal data is being collected by a corporation carrying out a research experiment.

In order to block bots, websites began turning to a software tool called CAPTCHA programs. First developed at Carnegie Mellon University in 2007, CAPTCHA is an acronym that stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart.[175] The test is named after Alan Turing, a groundbreaking World War II cryptologist whose work for the British government at Bletchley Park, helped the Allied forces crack the German Enigma codes, and, through that staggering mathematical achievement, helped turn the tide of the war.[176] It was Turing who first proposed, in 1950, a definition and standard for artificial intelligence. Under what has become known as the Turing test, a computer could be said to "think" if, in a conversation, a human being couldn't tell whether it

173. James O'Malley, *Captcha if you can: How you've been Training AI for Years without Realizing it*, TECHRADAR (Jan. 12, 2018), https://www.techradar.com/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it.

174. *Id.*

175. Mark Abadi & Samantha Lee, *11 Words you Probably didn't Know were Acronyms*, BUSINESS INSIDER (Aug. 6, 2019), https://www.businessinsider.com/acronyms-words-radar-taser-snafu-2018-6.

176. *Alan Turing Biography*, BIOGRAPHY (last updated Jul. 16, 2019), https://www.biography.com/scientist/alan-turing.

was interacting with another human being or with a computer.[177] In the paper, "Computing Machinery and Intelligence,"[178] Turing wrote, "I propose to consider the question, 'Can machines think?'"[179]

He suggested an experiment: if a person is having a disembodied conversation by means of teletype answers (or, today, through a computer screen), can the person tell whether they're interacting with a computer or another person?[180] Turing suggested that within fifty years it would no longer be necessary to guess what the outcome of the "imitation game" might be, because mathematics would have progressed so greatly that this question would no longer be a research hypothetical; we would be confronted with evidence of whether machines could mimic humans or not.[181]

Turing's prediction was prescient. By the end of the 20th century, computer scientists were taking a variety of approaches to constructing tests that would measure a computer's "artificial intelligence" against a variety of standards, including the one that Alan Turing had proposed.[182] Despite the ways in which AI research has branched out, the Turing test remains helpful background in understanding what CAPTCHA tests do on websites, and why they matter to a discussion about online behavior and personal data.

CAPTCHA tests proved to be so useful that the software behind them was purchased by Google in 2009, a mere 2 years after it was rolled out by the Carnegie Mellon computer scientists.[183] At the time, Google was in the process of digitizing its online library of books and needed humans to validate the text it was digitizing - to verify that particular text indeed represented particular words. This was part of the process of "education" for the computer that Alan Turing had first envisioned in his 1950 paper. CAPTCHA allowed Google to profit from both sides of a multi-sided transaction: Google needed human labor to validate the digital text and train its artificial intelligence algorithms to recognize similar text samples in the future. Websites that were being indexed by Google wanted a way to ensure that traffic directed to their sites – usually by Google – was human traffic, not bots. Google

177. Alan M. Turing, *Computing Machinery and Intelligence*, 59 MIND 433, 433–34 (1950)). In his famous paper from the time, Turing referred to this as "the imitation game," which also gave rise to the title for the 2014 movie in which Benedict Cumberbatch portrayed a young Alan Turing working at Bletchley Park at the height of the war. *See generally id.*

178. *Id.*

179. *Id.*

180. *Id.*

181. "I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted. . . . The only really satisfactory support that can be given for the view expressed at the beginning of sec. 6, will be that provided by waiting for the end of the century and then doing the experiment described." *Id.*

182. *See, e.g.*, Jia You, *Beyond the Turing Test: Concluding that there is no one test for Machine Intelligence, AI Researchers Develop a Battery of Research Challenges*, 347 SCI. MAG. 116 (2015).

183. O'Malley, *supra* note 174.

stood to profit if it could provide a security mechanism to weed out bot traffic from users who navigated to new sites by clicking on Google-offered links. The security check was yet another service that Google could provide to the users of the global internet. Google matched up the human users with the security they needed to access websites and matched up training data with people who were willing to train AI. This was partly because they did not know that was what they were doing when they completed a CAPTCHA request, and partly because they had no choice if they wanted to access the websites they were seeking to navigate to. It was an elegant, and potentially profitable, solution to what might otherwise have been two vexing problems.

Just as Turing had predicted, the AI began to learn and improve over time as it was trained on an ever-expanding library of validated data. Google renamed the software to reCAPTCHA and by 2012, it was so well trained on text data that it needed new challenges.[184] Google's AI began looking at mouse usage, site navigation, cookies, and other features of physical and virtual interaction with a site to predict whether a user was likely to be a human or a bot.[185] If the AI concluded the user was probably a human, then the "I am not a robot" checkbox appeared as an option, allowing the user to check the box, hit return, and proceed directly to the website they were seeking to access.[186]

For users whose activity was not sufficiently bland and consistent with both generic human activity and their own typical online behavior, reCAPTCHA began presenting new challenges, like choosing whether a photo included leaves or a cat.[187] By 2016, the person's action in tagging the cat photo helped add another marked photo to Google's library. The effect of adding another data point to all of the cat photos that were being used was to train Google's AI how to recognize a cat in the future when it came across an unfamiliar image.[188] By 2019, AI researchers are thinking about what the next type of test should be. In the short span of a

184. In the early 2000s, simple images of text were enough to stump most spambots. But a decade later, after Google had bought the program from Carnegie Mellon researchers and was using it to digitize Google Books, texts had to be increasingly warped and obscured to stay ahead of improving optical character recognition programs — programs which, in a roundabout way, all those humans solving CAPTCHAs were helping to improve." Josh Dzieza, *Why Captchas Have Gotten so Difficult*, THE VERGE (Feb. 1, 2019 11:00 AM), https://www.theverge.com/2019/2/1/18205610/google-captcha-ai-robot-human-difficult-artificial-intelligence.

185. *See, e.g.*, Andy Greenberg, *Google can now Tell you're not a Robot with Just one Click*, WIRED (Dec. 3, 2014 9:00 AM), https://www.wired.com/2014/12/google-one-click-recaptcha/; *see also* Katherine Schwab, *Google's new reCAPTCHA has a Dark Side*, FAST COMPANY (June 27, 2019), https://www.fastcompany.com/90369697/googles-new-recaptcha-has-a-dark-side.

186. *Id.*

187. *Id.*

188. "So it is hugely convenient then that Google has at its disposal hundreds of millions of internet users to work for it: by using Recaptcha (sic) to tackle these problems, Google can use our need to prove we're human to force us to use our very human intuitions to build its database." O'Malley, *supra* note 174.

decade, AI had advanced so substantially that machines were becoming almost as good at image recognition as people.

There would need to be something new, something that humans could do so much more effectively and accurately than machines that computers simply wouldn't be able to compete; they would quickly be spotted as imposters by anyone playing the game. Until then, however, our need to access secure websites will continue to create incentives for Google to develop tools to recognize and assess human behavior – tools that rely on factors that Google hasn't disclosed, but that likely have impacts to personal privacy.[189]

Where the survey economy collects detailed personal information in exchange for wages, the CAPTCHA and RECAPTCHA tests don't alert users that their labor is being used or that their data – in the form of mouse tracking and other behavior - is being collected without compensation to train data models for AI. The gig economy is facing the possibility of a range of reforms, with companies like Uber and Lyft having to face the possibility that their contract workers may be entitled to the hard-won benefits of regular employees.[190] But that road is a long and uncertain one, and it isn't clear that it will ever apply to the digital pieceworkers laboring away at giving up their personal data for cash. Here, too, there are parallels in history, as labor leaders and social advocates called for better wages and working conditions for the pieceworkers.[191]

As it turned out, however, collective bargaining was all but impossible for the seamstresses working in small groups or alone in their homes. The same challenges extend to digital piecework today, carried out in dorm rooms and apartments around the world. In some cases by people who don't care if they get paid for their data and who are filling out surveys for a lark, and in many other cases by people whose time is so undervalued by society that even a few cents is worth hours of labor. These are done in part to afford the disposable computers that they've purchased from a mobile phone provider on a 30-month installment plan.

The full implications of the intersection of personal data and workers in the gig economy are beyond the scope of this article. But digital piecework provides a useful illustration of how complicated the issues relating to data-driven technologies are, and how many disparate areas of law - currently scattered across

189. "Google is also now testing . . . a customized reCaptcha for enterprises that are looking for more granular data about users' risk levels to protect their site algorithms from malicious users and bots. But this new, risk-score based system comes with a serious trade-off: users' privacy." *See* Schwab, *supra* note 186.

190. Kate Conger & Noam Scheiber, *California Bill Makes App-Based Companies Treat Workers as Employees*, N.Y. TIMES (Sep. 11, 2019), https://www.nytimes.com/2019/09/11/technology/california-gig-economy-bill.html.

191. Social reformers, early labor leaders, and charitable organizations called for higher wages and better working conditions for seamstresses. Several newspapers took up their cause, exposing the harsh conditions in the needle trades. Reformers' attempts at establishing cooperatives in several cities aided some workers but achieved little permanent effect." Harris, *supra* note 140.

multiple Congressional committees - arise at this intersection. To further illustrate the point, it's worth taking a closer look at another dimension of the digital piecework phenomena, and the ways in which paid online surveys raise ethical concerns similar to those that prompt review by Institutional Review Boards ("IRBs") in more traditional research contexts.

A. Institutional Review Boards and Unconsenting Research Subjects

Traditional medical and social research has, for nearly half a century, been governed by a set of regulatory guidelines and a longstanding set of and processes designed to incorporate ethics review into experiments involving human subjects.[192] These ethical standards for human subject research have been in place in the U.S. for nearly a half-century, when the foundational principles were captured in a document known as The Belmont Report.[193] The "Common Rule" for human subjects research and the Institutional Review Board, or IRB, process that grew out of that report reflects a recognition of the inherent worth and dignity of each individual, and imposes a set of specific obligations on researchers who want to run experiments that involve individuals.

According to the U.S. National Institutes of Health, human subjects research is: "Research involving a living individual about whom data or biospecimens. . . are obtained, used, studied or analyzed through interaction/intervention, or where identifiable, private information is used, studied, analyzed, or generated is considered to involve human subjects."[194] This definition and associated rules are catalogued in a section of the U.S. Code of Federal Regulations titled "Protection of Human Subjects."[195]

Strictly speaking, the regulations only apply to research which is supported, funded or carried out by federal agencies or federally funded entities - which includes many traditional research organizations, like hospitals, medical researchers, and universities, but there have long been calls for the Common Rule ethical standards to be applied beyond the scope of federally funded research.[196]

---

192. "The Federal Policy for the Protection of Human Subjects or the "Common Rule" was published in 1991 and codified in separate regulations by 15 Federal departments and agencies." U.S. DEPT. OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html.

193. Belmont Report: Ethical Principals and Guidelines for the Protection of Human Subjects of Research, 44 Fed. Reg. 23192 (April 18, 1979).

194. *Frequently Asked Questions*, NIH GRANTS AND FUNDING, https://grants.nih.gov/policy/hs/faqs.htm#5772 (last visited Jan 9, 2019)

195. 45 C.F.R. pt. 46 (2009).

196. "Companies and other organizations may voluntarily choose to apply the Common Rule and/or other Subparts of 45 CFR 46 to their research projects. . . . The [Institute of Medicine] recommended that federal protections such as requirements for IRB approval and informed consent extend to every research project that involves human participants, regardless of funding source or research setting. [and the National Bioethics Advisory Commission] recommended a unified, comprehensive federal policy embodied in a single set of regulations and guidance that would apply to all types of research involving human participants (which would

The regulations define human subjects research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[197] The regulations govern collection of "identifiable private information" from individuals, where "private information" includes "information about a behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place" or "which the individual can reasonably expect will not be made public."[198] The regulations govern interventions, manipulation of the subject's environment, and interaction communication or interpersonal contact, and imposes an obligation to assess whether the research carries more than "minimal risk."

Under the regulations, an IRB may only approve research if all of the following criteria are satisfied: the research plan minimizes risks to participants; uses sound research design for its procedures; avoids exposing subjects to unnecessary risk; demonstrates that the risks to subjects are reasonable in relation to anticipated benefits, if any, to subjects, and in relation to the importance of the knowledge that may reasonably be expected to result; the selection of subjects is equitable; informed consent will be obtained; and there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of their data, including additional safeguards to protect the rights and welfare of; and if some or all of the subjects who are likely to be vulnerable to coercion or undue influence, additional safeguards have been included in the study to protect the rights and welfare of these subjects.[199] In nearly all cases, IRBs require researchers to obtain informed consent from research subjects, explaining, among other things, what the research will entail, what the risks are, whether and how their information will be kept confidential, explaining whether the individuals are likely to experience any benefit or harm from participating in the research, and informing them that they can withdraw from the research at any time without penalty.[200] The IRB must also assess whether there is a risk of more than minimal harm, and whether there is likely to be benefit to the individual data subjects.[201]

---

unify the requirements of Common Rule, FDA regulations and HIPAA)." ERIN D. WILLIAMS, CONG. RESEARCH SERV., RL32909, FEDERAL PROTECTION FOR HUMAN RESEARCH SUBJECTS: AN ANALYSIS OF THE COMMON RULE AND ITS INTERACTIONS WITH FDA REGULATIONS AND THE HIPAA PRIVACY RULE.

197. Definitions for Purposes of this Policy, 45 C.F.R. § 46.102 (2018)

198. "Human subject research means a living individual about whom an investigator (whether professional or student) conducting research: . . .(i) obtains information . . . through intervention or interaction with the individual, and uses, studies, or analyzes the information. . . or (ii) Obtains, uses, studies, analyzes, or generates identifiable private information." 45 C.F.R.§ 46.102(e).

199. *Id.* § 46.111.

200. *Id.* § 46.116.

201. *Id.* §§ 46.405–07.

In 2017, the federal government promulgated a major update to the Common Rule.[202] The final regulations articulated the rationale behind the update, which read in part:

> This final rule recognizes that in the past two decades a paradigm shift has occurred in how research is conducted. Evolving technologies—including imaging, mobile technologies, and the growth in computing power—have changed the scale and nature of information collected in many disciplines. Computer scientists, engineers, and social scientists are developing techniques to integrate different types of data so they can be combined, mined, analyzed, and shared. The advent of sophisticated computer software programs, the Internet, and mobile technology has created new areas of research activity, particularly within the social and behavioral sciences …The sheer volume of data that can be generated in research, the ease with which it can be shared, and the ways in which it can be used to identify individuals were simply not possible, or even imaginable, when the Common Rule was first adopted.[203]

The regulations provide a lengthy and complex set of rules that impose minimum baseline ethical standards for research that is supported by federal funding.[204] This article doesn't address those regulations in detail, nor attempt to parse the circumstances under which collection and analysis of survey data from or about individuals would fall within these regulations.[205]

Rather, the point of these examples has been to demonstrate that the widespread availability of personal data has made it possible for private sector actors to collect, analyze, and use vast quantities of personal data in ways that, if undertaken by scientists in more conventional, federally-funded research settings, would at least require analysis under the legal and ethical framework that's been established for human subjects research. When, however, the work is being performed solely by the private sector, very few constraints exist, either on the collection and use of the data itself, or on how those uses might impact the individual whose data is at issue. If these activities were subject to formal review, an IRB might question whether the data subjects have been informed and whether the benefit to them outweighs the harm of these activities, whether the activities

202. Federal Policy for the Protection of Human Services, 82 Fed. Reg. 12, 7149 (Jan. 19, 2017) (to be codified at 45 C.F.R. pt. 46).

203. *Id.*

204. Under the regulations that were in effect until 2018, the Common Rule applied to 19 federal agencies. Under the newly revised regulations, 20 federal agencies will follow the Common Rule. *See* 45 C.F.R. § 46 (2018).

205. The regulations provide an exemption for some types of research involving surveys, interviews, and observation of public behavior. *See* 45 C.F.R. §46.104(d)(2).

involve a massive market of unpaid labor, in example CAPTCHA, underpaid labor, in example Survey Junkie, and or other types of unrestricted and unethical social science research.

It's striking, perhaps, that Turing was criminally prosecuted and stripped of his livelihood for personal behavior of the very type that many people hope to keep private.[206] If Turing were alive and living in England today, he would no longer be prosecuted under criminal laws that have, thankfully, been repealed. But he might nonetheless prefer to keep his sexual behavior and relationships private. And that is something that, in today's data-intensive environment, is increasingly difficult to do.

Each of these examples illustrates different dimensions of the privacy-related issues that legislators ought to be equipped to consider in deciding what kinds of data-related laws to pass, and what those laws should cover. To the extent that Congress decides to consider legislative proposals relating to the survey economy, these disparate examples – involving marketing surveys and labor rates of pay, human subjects research, and collection and use of data and tasks to train AI without obtaining the data subjects' consent – provide a non-exhaustive sample of just a few of the kinds of issues. If these issues were to be considered on today's Congress, they would span across the jurisdiction of multiple committees.

VII. CONSUMER SURVEILLANCE: EAVESDROPPERS IN THE KITCHEN AND THE BABY'S ROOM

Personal digital assistants like Amazon's Echo, Google Home, and others are picking up audio and video feeds of previously-private moments in an increasing number of homes.[207] Smart security systems like Amazon Ring, Google Nest, and others are recording video, and sometimes audio, from both inside and outside an increasing number of homes and apartments. Sometimes capturing images not just of activity on the property itself, but of next door neighbors and passersby on the street or elsewhere beyond the property boundaries of the person who installed the smart security device.[208] The scope of data collection by these devices is still poorly

206. Turing was prosecuted for homosexual acts and ultimately passed away in what was deemed a suicide. *See supra*, note 177. Whatever one's definition of "privacy" might be, most people would agree that privacy ought to include granting individuals the to decide whether information about their sexual orientation or gender identity, their sexual behavior and intimate relationships, will be made public.

207. Lucas Matney, *More than 100 Million Alexa Devices Have Been Sold*, TECHRADAR (Jan. 4, 2019), https://techcrunch.com/2019/01/04/more-than-100-million-alexa-devices-have-been-sold/.

208. According to some market studies, it's estimated that 12.9 percent of all U.S. homes had some form of smart home security system in 2018. Cristoph Blumtritt, *Smart Home Penetration Rate Forecast by Country in the Segment Security 2018*, STATISTA (Nov. 20, 2019), https://www.statista.com/statistics/484294/smart-home-penetration-rate-for-selected-countries-in-the-segment-security/. By 2020, the number of people using smart security systems is expected to grow to over 22 million. Ronday Kaysen, *Do Security Systems Make you Safer?*, N.Y. TIMES (Dec. 22, 2017), https://www.nytimes.com/2017/12/22/realestate/do-security-systems-make-your-home-safer.html.

understood by many consumers, who sometimes believe that data is only recorded when the device receives a direct command.[209] On the contrary, much of this data – along with information from private company baby monitors, private home security systems, and others – is going directly into privately owned clouds.[210] The companies have full access to the data and consumers have to rely on the company's promises of reasonable data security and responsible use as their only assurances that the data won't be misused.[211]

Whether subpoenaed by law enforcement as evidence[212] in a crime or inadvertently forwarded to other users,[213] the data we provide to Alexa and Siri and the host of other digital assistants further adds to the complex picture of our everyday activities. There are very few limits on what data they can acquire, how long they can hold it, and what they can do with the information.[214] Even where legal limits exist, it's an open question whether individual consumers can meaningfully enforce their rights against these companies. And each of these devices presents even more complicated questions when it comes not to owners, but to their guests. Do homeowners have an obligation to tell their guests that an in-home security system is recording them? To tell the babysitter that the smart tv is watching them? To unplug their Echo when having a conversation with a friend at the kitchen table, and the friend thinks the conversation is confidential?

The growing popularity of smart devices, and the ever-expanding variety of types of smart devices, brings with it expanded opportunities for privacy issues to arise in what are, perhaps, unexpected ways, from baby monitors to children's toys and home security systems. There have been multiple accounts of hackers gaining access to baby monitors and redirecting the camera, including one in which the hackers remotely redirected the monitor's camera to take video of the parents' bed

209. *See, e.g.*, Geoffrey Fowler, *Alexa has Been Eavesdropping on you this Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/.

210. *Id.*

211. Matt Day et al., *Amazon's Alexa Team can Access Users' Home Addresses*, BLOOMBERG (Apr. 24, 2019 12:21 PM), https://www.bloomberg.com/news/articles/2019-04-24/amazon-s-alexa-reviewers-can-access-customers-home-addresses.

212. Tom Dotan & Reed Albergotti, *Amazon Echo and the Hot Tub Murder*, THE INFORMATION (Dec. 27, 2016 7:01 AM), https://www.theinformation.com/articles/amazon-echo-and-the-hot-tub-murder.

213. Geoffrey Fowler, *Hey Alexa, Come Clean About how Much you're Really Recording us*, WASH. POST (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/.

214. Some state legislatures have considered bills that would require consumer consent before smart speaker companies could store recordings, including the California Anti-Eavesdropping Act. AB 1395, Cal. State Leg., 2019-20 Sess. (2019); the Illinois Keep Internet Devices Safe Act, SB 1719, Ill. Gen. Assemb. 101st Gen. Assemb. (2019).

where the mother breastfed the baby and where the parents slept.[215] In late 2018, there were news reports that a man had hacked into a family's baby monitor and threatened the family.[216]

The privacy issues are wide-ranging apparently wide ranging. Video feeds going to peeping toms, and hackers using the camera to gain access to broader segments of the home Wi-Fi networks, potentially including access to computers and other kinds of accounts as well as to Wi-Fi enabled devices.[217] Why is it so easy? According to security researchers, many baby monitors lack the basic security controls that are built into other kinds of computing devices in important ways. In example hackers can automatically reset to factory default settings, which could have the effect of overwriting a custom-set password.[218] Sometimes these devices enable security settings to be bypassed altogether.

The South Carolina mother whose baby monitor kept redirecting its gaze from the baby's bassinet to the parents' bed is an example of this. The family had set a unique password for the baby monitor – but apparently that password was overridden or bypassed by whoever gained access to the controls for the camera's direction and feed.[219] As concerns about baby monitor privacy have grown, tech publications and parenting websites have taken to posting reviews of the relative security of various makes and models of baby monitor.[220] Several outlets are publishing articles on how to implement more effective security settings,[221] and at least one toy maker scaled back its plans for an internet-connected baby monitor over privacy concerns raised by parents and legislators alike.[222]

The challenge isn't limited to baby monitors; cameras are increasingly embedded in children's toys as well.[223] In 2017, the German government urged parents to

215. Camila Domonoske, *S.C. Mom Says Baby Monitor Was Hacked*, NPR (June 5, 2018, 7:18 PM), https://www.npr.org/sections/thetwo-way/2018/06/05/617196788/s-c-mom-says-baby-monitor-was-hacked-experts-say-many-devices-are-vulnerable.

216. Amy Wang, *I'm in your Baby's Room: A Hacker took over a Baby Monitor and Broadcast Threats, Parents say*, WASH. POST (Dec. 20, 2018 1:55 Pm), https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/.

217. *Id.*

218. *Id.*

219. *Id.*

220. *See, e.g.*, *Which Baby Monitor is Safe from Hacking*, KID SAVERS NETWORK, https://kidsaversnetwork.com/newborn/which-baby-monitor-is-safe/.

221. See, for example, *Can Digital Baby Monitors Be Hacked? Learn How to Protect Your Privacy*, BABY GEAR ESSENTIALS, https://babygearessentials.com/hacked-baby-monitor/; and Lisa Vaas, *How to Secure your Baby Monitor*, SOPHOS (Apr. 24, 2015), https://nakedsecurity.sophos.com/2015/04/24/how-to-secure-your-baby-monitor/.

222. Energy & Technology Editorial Staff, *Mattel Spikes Smart Baby Monitor Amid Privacy Concerns*, ENG'G. AND TECH., https://eandt.theiet.org/content/articles/2017/10/mattel-spikes-smart-baby-monitor-amid-privacy-concerns/.

223. This holiday shopping season, millions of parents will consider purchasing "smart" toys for their children. These "connected toys – toys that are connected to the internet – offer many promising applications,

destroy the "My Friend Cayla" doll, warning parents that the doll could be used as a spy camera to take video and audio recordings of unsuspecting children, without the knowledge or consent of the children or their parents.[224] The doll can be controlled by an app, and uses speech recognition software to allow children to access the internet.[225] But these features – while carrying a certain "gee whiz" panache in the U.S. where the toymaker, Genesis Toys, is based – prompted German regulators to declare the doll an "illegal espionage apparatus" under laws that prohibit surveillance devices in Germany from being disguised as other objects.[226] The ban by German regulators was a fascinating one because of the tensions it brought to light between national regulations that are designed to protect privacy, and the individual consumer preferences that are sometimes at odds with the laws that purport to protect them. In the case of Cayla, those tensions were on full display. The German laws that Cayla violated didn't just prohibit manufacturers from creating deceptive devices, or items that appeared to be ordinary objects but that had surveillance capabilities. The law made it illegal to manufacture, sell, or possess any such devices.[227] Once Cayla was declared to be such a device, the tension came into full view.

Cayla had a great many vulnerabilities. According to critics, access to the doll was "completely unprotected," as it did not even require a simple password to access it and its Bluetooth signal could be hacked from 50 feet away. This allowed a hacker to listen to the child's conversations with the doll, and even to talk to the child through the doll's embedded speakers.[228] However, it clearly had wide commercial appeal. Cayla had been named a "top ten" toy of 2014 by a German toy trade organization.[229] Because it is illegal to possess disguised surveillance devices, in theory it would be possible for the government to prosecute families for having a Cayla doll in their homes.

Cayla is hardly the only instance of a poorly protected internet-connected toy. The Cloud Pets toys that allowed children to send and receive audio messages were pulled from stores after security researchers discovered a serious security flaw. Children's names, ages, and voice recordings were easily accessible on the internet because the manufacturer had failed to implement password-protection on the

---

including the potential to assist in the overall education and cognitive development of children. The personally identifiable information (PII) collected by these connected toys, however, also raises serious privacy and data security concerns." COMMITTEE ON COM., SCI., AND TRANS., 114th CONG., CHILDREN'S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS (2016).

224. Philip Oltermann, *German Parents Told to Destroy Doll that Can Spy on Children*, THE GUARDIAN (Feb. 17, 2017, 11:53 AM), https://www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children.

225. *Id.*

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

cloud system where records, including audio files, from and about the children using the toys were stored.[230] Another example, the Fisher-Price Smart Toy Bear, a wi-fi connected stuffed animal, was marketed to consumers as "an interactive learning friend that talks, listens, and remembers what your child says and even responds when spoken to."[231]

According to a Senate report, security researchers discovered a security vulnerability that would make it possible for hackers to access the smart toy server and view children's information, and even take over control of the toy.[232] The same report also described the vulnerabilities found in a children's GPS tracking watch that made it possible for hackers to gain unauthorized access to the location information of the children wearing the devices and the family members who had joined a the group location sharing feature offered by the watch's app.[233] In a different kind of privacy incident, the 2015 cyberattack on the network of toy company VTech allowed hackers to gain access to the home addresses, and photographs of over six million children.[234] In recognition of these risks, the FBI issued a public service announcement ("PSA") in 2017 warning about the privacy risks of internet-connected toys.[235] According to the release,

> The FBI encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments. … These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS option. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.[236]

Although the FBI points to the risk of what it refers to as "child identity fraud,"[237] the other dangers described in the PSA are far more chilling. The PSA points out that in some cases, toys' microphones can record and collect conversations that are within earshot, and that

230. Diane Shipley, *Reminder: Smart Toys Are Cute, Cuddly, and Full of Security Risks*, MASHABLE (Jan. 26, 2019), https://mashable.com/article/smart-toys-security-privacy/.

231. *See supra,* note 224, at 12.

232. *Id.* at 13.

233. *Id.* at 15. *See also* Mark Santislay, *R7-2015-27 and R7-2015-24 Fisher-Price Smart Toy hereO GPS Platform Vulnerabilities (FIXED)*, RAPID 7: BLOG (Feb. 2, 2016), https://blog.rapid7.com/2016/02/02/security-vulnerabilities-within-fisher-price-smart-toy-hereo-gps-platform/.

234. *Id.*

235. FED. BUREAU OF INVESTIGATION, PUB. SERV. ANNOUNCEMENT NO. I-071717 (REVISED), CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN (July 17, 2017).

236. *Id.*

237. *Id.*

> Information such as the child's name, school, likes and dislikes, and activities may be disclosed through normal conversation with the toy or in the surrounding environment. . . In addition, companies collect large amounts of additional data such as voice messages, conversation recordings, past and real-time physical locations, Internet use history, and Internet addresses/ IPs.[238]

As a result, "the potential misuse of sensitive data such as GPS location information, visual identifiers from pictures or videos, and known interests to garner trust from a child could present exploitation risks."[239] As it turns out, even security systems can backfire, as in the 2019 incident in which an unauthorized user gained audio and video access to an Amazon Ring camera installed in a children's bedroom, and used that access to harass the family's eight year old daughter.[240]

Smart home security systems have prompted other concerns as well. Civil liberties groups have objected to the widespread sharing of Amazon Ring video surveillance with police departments around the country.[241] The popular security cameras are intended to record video in the area surrounding the door to an apartment or home, but their field of view often extends far beyond a front stoop, recording actions and interactions of residents and passersby, many of whom may not suspect that their actions are being surveilled.[242] The surveillance isn't limited to cameras installed on individual homes, but can also be carried out as a group effort, as homeowners' associations install security cameras to monitor community streets.[243] Although current Fourth Amendment jurisprudence generally permits law enforcement to obtain information from third parties without a warrant under the Third Party doctrine,[244] several of the opinions in a 2018 Supreme Court decision have called into question whether the Third Party doctrine should be modified or altogether cast aside.[245]

---

238. *Id.*

239. *Id.*

240. Allyson Chiu, *She installed a Ring Camera in her Children's room for 'Peace of Mind.' A Hacker Accessed it and Harassed her 8-year-old daughter*, WASH. POST (Dec. 12, 2019), https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/.

241. Drew Harwell, *Doorbell-Camera firm Ring has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach/.

242. *See, e.g.*, Louise Matsakis, *The Ringification of Suburban Life*, WIRED (Sept. 26, 2019), https://www.wired.com/story/ring-surveillance-suburbs/.

243. *See, e.g.*, Megan Wollerton, *Neighborhood Security Cameras Sacrifice to Solve Crimes*, CNET (Mar. 27, 2018), https://www.cnet.com/news/neighborhood-security-cameras-sacrifice-privacy-to-solve-crimes/.

244. See United States v. Miller, 425 U.S. 435 (1976); and Smith v. Maryland, 442 U.S. 735 (1979).

245. *See generally* Carpenter v. United States, 585 U.S. 138 S. Ct. 2206 (2018).

This small sampling of privacy issues arising from data-driven consumer devices further illustrates the challenge for Congress in determining how to investigate and legislate these devices and their risks. Certainly, the House and Senate Commerce Committees have jurisdiction to review the privacy risks associated with these products. But some aspects of surveillance that these products make possible – like sharing of home video surveillance data with police – is a matter whose implications fall squarely within the scope of the Congressional Judiciary committees. As with other areas of data-driven technology, assessing the full privacy and other implications of smart consumer products not only is likely to cross committee jurisdictional lines; it is likely that Congress could be more effective, and better equipped, to assess the full range of potential issues if it had the benefit of a standing committee able to review these concerns through a comprehensive lens that takes into account multiple areas of law.

VIII. ARTICLE III STANDING DECISIONS IN PRIVACY CASES SHOW THAT DEFINITIONS OF COMPENSABLE HARM REMAIN UNCLEAR

There is a deep and significant split among federal circuits on the question of standing for data privacy cases, in which the standing analysis rests primarily on the question of whether various types of data breaches, or unauthorized access to personal information, constitute a compensable harm under applicable law.[246] Under the lines of case law interpreting *Spokeo v. Robbins*,[247]security breaches involving qualitative information such as photographs, user profile behavior and biometric information are frequently not recognized as compensable harms under U.S. law, even when the alleged harms take place in violation of a statute.[248]

In *Spokeo*, the Supreme Court held that in actions under federal statutes, a bare statutory violation is not enough by itself to provide a plaintiff with standing to sue.[249] Instead, drawing from a substantial body of federal jurisprudence, the *Spokeo* Court held that in order to meet the minimum standard for standing to sue under Article III of the Constitution, an injured plaintiff must show that the injury is both concrete and particularized, that it is actual or imminent, and that it is not

246. *See, e.g.*, Reilly v. Ceridian Corp., 664 F. 3d 38 (3d Cir. 2011); Remijas v. Neiman Marcus, 341 F.Supp. 3d 823 (7th Cir. 2015); Dieffenbach v. Barnes & Noble, 887 F.3d 826 (7th Cir. 2018); Galaria v. Nationwide Mutual Insurance Co., Nos. 15-3386/3387, unpublished (6th Cir. 2016); In re SuperValue, Inc., 925 F.3d 955 (8th Cir. 2017); Whalen v. Michaels Stores, Inc., 689 Fed.Appx. 89 (2nd Cir. 2017); Attias v. Carefirst, 865 F.3d 620 (D.C. Cir, 2017); Beck v. McDonald, 848 F.3d 262 (4th Cir. 2017); Hutton v. Nat'l Bd. of Exam'r in Optometry, Inc., No. 17-1506 (4th Cir. 2018); In re Zappos.com, Inc., 893 F.Supp.2d. 1058 (9th Cir. 2018); and Patel v. Facebook, No. 18-15982 (9th Cir. 2019).

247. 136 S. Ct. 1540 (2016).

248. *See, e.g.*, Strebel v. Comenity Bank, 842 F.3d 181 (2d Cir. 2016); Norberg v. Shutterfly, 152 F. Supp. 3d 1103 (N.D. Ill. 2015); McCollough v. Smarte Carte, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016); Vigil v. Take Two Interactive Software, Inc, 235 F. Supp. 3d 499 (S.D.N.Y. 2017), *aff'd in part and vacated in part sub nom*; Santana v. Take Two Interactive Software, Inc., 717 F. App'x 12 (2d Cir. 2017).

249. *Spokeo*, 136 S. Ct. at 1550.

conjectural or hypothetical, none of which can be shown by a "bare procedural violation" of a statute.[250] Standing can be even more difficult to demonstrate when the alleged injury doesn't arise from violation of a statute, but from violation of a company's privacy policy or terms of use.[251] Recent cases from the Illinois Supreme Court and the 9th Circuit have found compensable harm resulting from the violation of the Illinois Biometric Information Privacy Act.[252] The analysis in both cases rested squarely on the demonstrated intent of the Illinois legislature, as captured in both the legislative history and the language of the statute, to recognize the important privacy interests that individuals have in their biometric information.[253]

When VTech suffered the data breach that exposed children's personal information, the U.S. Federal Trade Commission, currently the nation's top watchdog for privacy matters, stepped in to investigate.[254] The result of that investigation was a settlement in which VTech agreed to pay a $650,000 fine to the government for violating COPPA.[255] Specifically, for failing to provide notice and obtain parental consent prior to collecting personal information from children, and for failing to take "reasonable and appropriate data security measures" to protect

250. *Id.* at 1548–50.

251. This issue is currently being litigated in the 9th Circuit, in the consumer class action lawsuit brought against Facebook for sharing users' profile information with political consulting firm Cambridge Analytica. In a September, 2019 ruling, Judge Vincent Chhabria of the northern District of California ruled that plaintiffs' case could proceed, despite defendant Facebook's arguments that: 1) users "have no legitimate privacy interest in information they make available to their friends on social media; 2) that "even its users had a privacy interest in the information they made available only to friends, there is no standing to sue in federal court because there were no tangible negative consequences from the dissemination of this information;" and 3) that "even if users retained a privacy interest in the information that was disclosed, and even if a 'bare' privacy invasion confers standing to sue in federal court, this lawsuit must be dismissed because Facebook users consented, in fine print, to the wide dissemination of their sensitive information." Mot. to Dismiss at 1-2, In re: Facebook, Inc. Consumer User Privacy Profile Litigation, 402 F.Supp.3d 767 (2019).

252. The Illinois Biometric Information Privacy Act is codified at 740 ILL. COMP. STAT 14/1 *et seq*. (2019). *See* Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan 25, 2019); *see also* Patel v. Facebook, 932 F.3d 1263 (2019). The complaint in *Rosenbach* was filed in the Circuit Court of Lake County, Illinois in January 2016. *See* Complaint, *Rosenbach*, 2019 IL 123186. The complaint in *In re Facebook* was filed in the Northern District of California in August 2015. *See* Complaint, *In re* Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 17, 2015).

253. *See generally Rosenbach*, 2019 IL 123186. Looking at the important interests that BIPA protects, the *Rosenbach* court found that "It is clear that the legislature intended for this provision to have substantial force. … To require individuals to wait until they have sustained some compensable injury beyond violation of their statutory rights before they may seek recourse, as defendants urge, would be completely antithetical to the Act's preventive and deterrent purposes." *Id.* at 9.

See also Patel, 932 F.3d at 18 (concluding "that 'the statutory provisions at issue' in BIPA were established to protect an individual's 'concrete interests' in privacy, not merely procedural rights").

254. *Electronic Toy Maker Vtech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act*, FED. TRADE COMM'N (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

255. *Id.*

the personal data that VTech was collecting.[256] The settlement also includes a consent decree; an agreement through which VTech is required to demonstrate its compliance with certain basic levels of data privacy protection, and to submit to oversight from the FTC to verify that the company is living up to its promises to implement more rigorous data privacy practices in the future.[257] Although the consent decree can, if aggressively monitored by the FTC, have real teeth in its impact on the company, and although the amount of the fine was significant, it's an open question as to how much a privacy violation should be worth. Additionally, it must be determined whether the violation will be measured by the number of children and families affected, or by the revenue, profits, or other measure of wealth of the company. In the VTech case, VTech was accused of collecting data without proper notice and consent from some three million children, with records from hundreds of thousands of those accounts compromised when hackers accessed the VTech customer-data storage system.[258] The same year as the hack, 2015, VTech reported revenue of over fourteen billion dollars, and in 2018, the year that the settlement agreement with the FTC was reached, VTech reported over sixteen billion dollars in earnings according to MarketWatch.[259] With the $650,000 fine amounting to a small fraction of that annual sales revenue, it's hard to know whether a fine of this magnitude amounts to a true deterrent, or is little more than the cost of doing business.

Although laws like COPPA provide some privacy protection for children, and FTC investigations and enforcement actions present a risk to companies and give them reason to be diligent in how they handle data, none of those measures help to compensate the children or parents. These individuals are the people whose personal information has been scooped up in ways they didn't imagine, or shared with third parties they didn't expect, or used to create personal profiles that form the basis for future commercial advertising and other marketing. Congress's role in privacy interests becomes particularly evident in the context of cases like those cited above, which demonstrate the ways in which various courts have grappled with the issue of standing and harm in data privacy and security litigation. Where some courts have recognized that privacy interests stem from, and are tied to, multiple sources of law, including common law, constitutionally protected zones of privacy, the Fourth Amendment, and statutes,[260] other courts have taken a narrower view.[261]

256. *Id.*

257. *Id.*

258. *Id.*

259. *Annual Financials for VTECH Holdings Ltd. ADR*, MARKETWATCH (2018), https://www.marketwatch.com/investing/stock/vtkly/financials.

260. *See Patel*, 932 F.3d at 1272–73 (discussing the importance of each of these sources of law in its analysis).

261. *See, e.g.*, Reilly v. Ceridian, 664 F.3d 38 (2011); *see also In re* Supervalu 870 F.3d 763 (2017).

While the existing Circuit split may be resolved in part if the Supreme Court granted certiorari in cases that are likely to help clarify these differing interpretations of *Spokeo's* applicability, Congress has the opportunity to play an equally important and potentially more immediately clarifying role. If Congress were to pass federal privacy legislation which includes both legislative history and legislative text clarifying the extent to which Congress intends to recognize substantive rights versus procedural requirements, that legislation could provide useful and effective clarity for companies, for individuals, and for future courts and litigants. In order to do that effectively, however, Congress would do well to consider the same wide-ranging scope of sources for privacy interest that have been recognized elsewhere, such as by the Ninth Circuit in Patel.[262]

Questions concerning the Fourth Amendment more typically arise in the Congressional judiciary, intelligence, and homeland security committees. Issues involving Constitutionally protected zones of privacy may arise in Congressional committees addressing health-related issues. Consumer protection issues often arise in the Congressional commerce committees, but may arise elsewhere as well.[263] Congress would be better postured to carry out a holistic review of the various dimensions of privacy-related interests, to make reasoned judgments about what capabilities of data-driven technologies intersect with individuals' substantive privacy and related interests, and to craft legislation that makes sensible distinctions between substantive rights and procedural requirements if the Congressional committee process was better organized to bring together the necessary perspective to assess the wide-ranging nature of privacy interests and concerns,

IX. ELECTION SECURITY AND POLITICAL INTERFERENCE

In recent years, online propaganda techniques have been used to influence everything from the public response to protests in Ferguson, Missouri and Baltimore, Maryland, to the Brexit vote in Britain, to the 2016 U.S. Presidential election, and to the elections in Germany and France in 2017 and 2018.[264] Social media platforms became a hotbed of propaganda activity and fake news that was propagated by automated bots, human trolls, and a nearly endless supply of posts.[265] What made these influence campaigns so successful, however, wasn't the mere fact of posting articles or ads. It was the use of individuals' personal data to create detailed, micro-targeted messages, to direct ads, pages, posts and other content specifically to users who would be most susceptible to its messages and in

262. *See Patel*, 932 F.3d at 1272–73.

263. For example, the use of smart speakers in classrooms raises issues that might be addressed by Congressional committees with jurisdiction over education.

264. 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 20 (2019), https://www.justice.gov/storage/report.pdf.

265. *Id.*

the places that mattered the most. Social media manipulators are using our own personal data as the most formidable weapon against us, and apparently to great effect.

In March 2019, Robert Mueller's Office of Special Counsel released a two-volume report on Russia's interference with the 2016 U.S. Presidential election.[266] Based on nearly two years of investigation, Mueller and his team concluded that "The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[267] One prong of that interference was an "active measures" campaign involving the use of fake social media accounts to sway opinion in the U.S.[268] Specifically, the Russian government worked through a St. Petersburg-based troll farm doing business as a company called the Internet Research Agency ("IRA"), run by a close associate of Russian President Vladimir Putin.[269] The IRA active measures efforts began in 2014, with IRA employees visiting the U.S. to carry out reconnaissance, and very quickly thereafter establishing fake accounts on Facebook, Instagram, Twitter, and other social media platforms.[270] "By the end of the 2016 U.S. election," notes the report, "the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants… Facebook estimated the IRA reached as many as 126 million persons through its Facebook accounts."[271] All of these accounts were designed to appear as if they were legitimate accounts associated with real U.S. people.[272] This Russian intelligence operation is an important story in geopolitical affairs generally, as it provides a stark example of the Kremlin's escalation of the types of political interference that it has engaged in for years via more traditional means.[273] However, for purposes of this article, a key feature of that active measures

266. *Id.*

267. *See id.* at 1.

268. *Id.* at 14.

269. *Id.*

270. 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14-15. (2019), https://www.justice.gov/storage/report.pdf.

271. *Id.*

272. "Masquerading as Americans, these [Russian] operatives used targeted advertisements, intentionally falsified news articles, self-generated content, and social media platform tools to interact with 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." 2 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14–15. (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

273. "The Committee found that Russia's targeting of the 2016 U.S. presidential election was part of a broader, sophisticated, and ongoing information warfare campaign designed to sow discord in American politics and society." Id., at 5. "Russia's intelligence services have been focused for decades on conducting foreign influence campaigns, or "active measures" and "disinformation." *Id.* at 11.

campaign is the fact that the IRA actively leveraged the personal data profiles available through social media platforms to target its advertising towards its intended audience.

According to the Senate Intelligence Committee's Report, "The IRA used Facebook's geographic targeting feature to channel advertisements to intended audiences in specific U.S. locations. About twenty-five percent of the advertisements purchased by the IRA were targeted down to the state, city, or in some instances, university level. Specific content narratives emerge[d] in connection with targeted locations."[274] The report notes that the social media platforms make available tools that could have allowed even more granular advertising, and a more focused attempt to direct specific messages to particular audiences, all based on the rich and complex personal data profiles that Facebook builds on its users; had the IRA done so, their manipulative and divisive social and political messages might have had even greater impact. According to the SSCI report, "Facebook indicates that the IRA did not leverage the platform's Custom Audiences tool, which would have entailed uploading or importing an externally held list of advertisement targets or contact data, revealing the IRA's efforts were not as effective as they could have been."[275]

The fake identities for the accounts varied widely. For example, one of the most widely followed IRA trolls was a Twitter account with the handle @TEN_GOP – an account that fooled hundreds of thousands of Twitter users into believing that it was an "unofficial account" of the Tennessee Republican party. Another account, @Jenn_Abrams, famously duped her 70,000 Twitter followers and countless other Twitter users who interacted with her content: Roseanne Barr argued with her on Twitter, a celebrity news outlet called Brit & Co wrote a whole article about the troll account's tweets on Kim Kardashian. [276] The fake account posed tweets about pop culture, ballistic missiles, the Confederate flag, and Rachel Dolezal.[277] Her tweets were featured in articles in USA Today, the New York times, The Daily Caller, Buzzfeed, and a host of other U.S. and international news outlets.[278] Abrams followed a modus operandi common to many of these troll accounts: build up a following with an entertaining and engaging online persona that posted content about nonpartisan issues – celebrity gossip, general news – and then, after attracting a substantial following, start pushing out deeply divisive content on wedge issues in American politics, like immigration, race, and gay rights and, closer to the 2016 election, content deeply critical of, or spreading conspiracy theories

274. *Id.* at 44–45.

275. *Id.* at 45.

276. Ben Collins & Joseph Fox, *Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World*, THE DAILY BEAST (Nov. 2, 2017, 8:00 PM), https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

277. *Id.*

278. *Id.*

about, Democratic nominee Hilary Clinton.[279] Abrams was particularly successful at creating a total package of a person; in addition to her Twitter, she also had a personal website, a Medium page, a Gmail address, and a GoFundMe page.[280]

A research study recently published in the Columbia Journalism Review concluded that most major news outlets had at some point in time unknowingly quoted Russian hoax accounts, usually in stories reporting on public reaction to recent public events or controversies in the news.[281] Perhaps not surprisingly, news outlets with a more left- or right-leaning bent were more likely to report on the often incendiary social media posts: The Daily Caller and Huffington Post were the outlets that most frequently published quotes from fake social media accounts.[282] But the challenge of differentiating authentic accounts from fake ones – the problem of differentiating the true from the false, hit major mainstream news outlets in the center of the political spectrum as well, including such highly regarded ones as The New York Times, NPR, and the Washington Post.[283]

Neither the criminal indictments against the IRA nor the widespread news coverage about Russia's fake social media profiles and influence campaign seem to have had any deterrent effect. It is now widely believed that the Russian government carried out similar influence operations in the run-up to Great Britain's Brexit vote.[284] More recently, Russia's troll farms were accused of attempting to influence the presidential election in France,[285] the German prime minister election in 2017,[286] and of stoking France's "yellow vest" protests in 2018.[287] Russian troll farms were implicated in using Facebook, Twitter and YouTube accounts in their attempts to sway European Union elections in 2019.[288] The playbook was the same as it had been in the U.S. in 2016: suppress voter turnout, deepen political divides, and advance a far-right policy agenda through fake accounts, disinformation, and the exploitations of local political divisions that were already existing. Adding insult

279. *Id.*

280. *Id.*

281. Josephine Lukito & Chris Wells, *Most Major Outlets Have used Russian Tweets as Sources for Partisan Opinion Study*, COLUM. JOURNALISM REV., (Mar. 8, 2018), https://www.cjr.org/analysis/tweets-russia-news.php.

282. *Id.*

283. *Id.*

284. *See generally Foreign Influence in Political Campaigns*, UK PARLIAMENT, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179109.htm.

285. *See, e.g.*, Erik Brattberg & Tim Maurer, *Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks*, CARNEGIE ENDOWMENT (May 23, 2018), https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

286. *See, e.g.*, Naja Bentzen, *Foreign Influence Operations in the EU* (2018), http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/625123/EPRS_BRI(2018)625123_EN.pdf.

287. *See, e.g.*, Luke Coffey, *Russia Exploits "Yellow Vest" Turmoil in France*, THE HERITAGE FOUNDATION (Feb. 8, 2019), https://www.heritage.org/europe/commentary/russia-exploits-yellow-vest-turmoil-france.

288. *See* Adam Satariano, *Russia Sought to Use Social Media to Influence E.U. Vote, Report Finds*, N.Y. TIMES, (Jun. 14, 2019), https://www.nytimes.com/2019/06/14/business/eu-elections-russia-misinformation.html (explaining voters in Britain, France, Germany, Italy, Poland and Spain were among those targeted).

to injury, in 2019, a Russian troll farm that was a close cousin to the IRA, the Federal Agency of News, had the temerity to file a lawsuit in U.S. federal court, charging Facebook with violating its First Amendment rights for expelling it from Facebook.[289]

Reports from the UK Parliament have laid out in excruciating detail the ways in which social media disinformation is fueling social discord and political divisiveness, as well as uninformed or misinformed political thinking.[290] The Australian Competition and Consumer Commission has issued a report from its social media inquiry describing the ways in which social media platforms are not only spreading misinformation, but also driving legitimate news outlets, such as newspapers, with a history of employing local journalists, informing the public about local news, and carrying out rigorous fact checking – out of business.[291]

The societal risks aren't simply that traditional journalism is, to some extent, being displaced by ever-more fringe news outlets offering skewed content on the right and the left of the political spectrum. This trend does, to be sure, accelerate the tendency for people to get caught in their own news echo chambers and may make critical thinking about controversial or emotionally charged issues more difficult. As troubling as the social and political impacts of those facts might be, the more pernicious fact of social media's role in this shifting journalistic landscape is that social media makes it so easy to feed the trolls. Because social media platforms know so much about our individual behavior, interests, personality traits, and inclinations, and because of the way that their advertising and engagement models work, social media platforms present a nearly-ideal mechanism for people with a message, including people with messages that may be distorted, damaging, false, or divisive message. Social media enables people, companies, and countries to individually target their content towards each user of a social media platform, and therefore to each prospective voter. A hypothetical example helps illustrate the risk: A single Russian troll might target content to me and to my husband on social media; however, they will use different content to do it. Different memes. Different invitations to group pages. Different appeals to our emotions. Different advertising. This is for a simple reason: my husband and I have different personality traits and different interests, and the social media platforms make it easy to micro-target different audiences with different messaging, all designed to have maximum

289. Specifically, the Federal News Agency filed a lawsuit against Facebook, claiming that Facebook was trying to silence a legitimate news organization and deter free speech. Anna Kaplan, *Judge Tosses Russian Trolls' Free Speech Lawsuit Against Facebook*, THE DAILY BEAST (Jul. 20, 2019, 11:20 PM), https://www.thedailybeast.com/judju-tosses-russian-trolls-free-speech-lawsuit-against-facebook. The Federal News Agency had previously been blacklisted by the United States for 2016 election interference. *Id.* The lawsuit was dismissed without prejudice by the San Jose Superior District Court. *Id.*

290. *See* COMMITTEE OF CULTURE, MEDIA AND SPORT, FINAL REPORT ON DISINFORMATION AND 'FAKE NEWS', HOUSE OF COMMONS (2019).

291. AUSTRALIAN COMPETITION AND CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY: FINAL REPORT 2019, https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report.

impact on the particular individual who sees the targeted content appear in their social media feed. Although the messaging might be tailored, in the case of foreign influence operations, the intended outcomes are almost always the same. Increase citizen dissatisfaction with life in the U.S., sow discord, undermine trust in democracy, explicit and exacerbate existing divisions in society, suppress voter turnout among key constituencies, and increase the odds that the foreign power's preferred candidate will win.

Think tanks like the Alliance for Securing Democracy at the German Marshall Fund have pointed to the destabilizing effect across all of the western democracies of authoritarian and nationalist movements that are being fueled in part by information operations that include these individually-directed and microtargeted political messaging.[292] Academics like Briony Swire-Thompson at Northeastern University and Kathleen Hall Jamison at University of Pennsylvania have done extensive research on the phenomena of fake news, Russian troll farms, and targeted social media political advertising.[293]

Jamieson, a prominent expert in public policy and political communications strategies, was one of the first to do comprehensive social science analysis of the impact that Russia's information operations on the 2016 U.S. elections.[294] Her conclusion: the Russian active measures campaign was powerful and effective in shaping U.S. public opinion, and likely changed the outcome of the election in favor of Donald Trump.[295] Swire-Thompson's research has a somewhat different focus, examining the cognitive mechanisms behind our susceptibility to "fake news."[296] In one of her recent papers, she notes that when people are attempting to assess the trustworthiness of information, we too often default to cognitive biases like, "they might be a liar, but they're my liar."[297]

In casting about for solutions, some advocates have suggested there should be laws requiring greater transparency in social media content, such as that suggested under the Honest Ads Act,[298] which would require political advertising to carry affiliation disclosure statements much like those that are required for political

292. *See Mission Statement*, ALLIANCE FOR SECURING DEMOCRACY: ABOUT US, https://securingdemocracy.gmfus.org/about-us/ (last visited Sept. 14, 2019) (recognizing that Russia's efforts to "sow and exploit divisions" through political messaging campaigns have the potential to weaken democratic institutions worldwide).

293. *See, e.g.*, Nir Grinberg et al., *Fake news on Twitter During the 2016 U.S. Presidential Election*, 363 SCIENCE 375 (2019). *See also* KATHLEEN HALL JAMIESON, CYBERWAR: HOW RUSSIAN HACKERS AND TROLLS HELPED ELECT A PRESIDENT: WHAT WE DON'T, CAN'T AND DO KNOW (Oxford Univ. Press 2018).

294. JAMIESON, *supra* note 294.

295. *Id.* at 1–17.

296. See generally the list of publications at BRONY SWIRE THOMPSON, https://brionyswire.com/.

297. *See generally*, Briony Swire-Thompson, et al., *They Might Be a Liar but They're My Liar: Source Evaluation and the Prevalence of Misinformation*, POL.PSYCHOL.(2019), https://brionyswire.files.wordpress.com/2019/07/pops_2019.pdf.

298. Honest Kids Act, S. 1356, 116th Cong. (2019).

advertising on radio or television.[299] Others have correctly pointed out that much of the false and misleading content that gets shared does not spread through paid advertising, but through inauthentic pages and accounts that misrepresent who the user is.[300] Many of the observers of this trend have suggested that the answer is to pass laws requiring social media platforms to engage in more content moderation, flagging bots and trolls, taking down inauthentic accounts, and removing offensive content.[301] That last prong – deciding when to take down content – runs into problems with both the principles of free speech protected by the First Amendment, and also with the current statutory framework[302] for internet regulation, under which platforms aren't considered publishers of the content posted by their users. Others focus on the need to emphasize critical thinking skills in school – but overlook the fact that research has shown that younger people are generally more savvy about the need to be skeptical of internet content, and that it's actually older voters who are far more likely to be swayed by slanted content or deceived by outright falsehoods when they are posted online.[303] According to some studies, older Americans are disproportionately likely to share fake news on Facebook; no matter what their gender, education level, or frequency of sharing activity was, age was more accurate than any other variable in predicting the likelihood that a person would share fake news.[304]

There are promising examples of how other countries are working to mitigate the societal impacts of social media disinformation and other kinds of propaganda campaigns being directed at the U.S. by foreign adversaries.[305] In the meantime,

---

299. *Id.*

300. "Initially, the IRA created social media accounts that pretended to be the personal accounts of U.S. persons. By early 2015, the IRA began to create larger social media groups or public social media pages that claimed (falsely) to be affiliated with U.S. political and grassroots organizations." 1 ROBERT S. MUELLER, III, U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 20 (2019), https://www.justice.gov/storage/report.pdf. "The Committee found that paid advertisements were not key to the IRA's activity, and moreover, are not alone an accurate measure of the IRA's operational scope, scale, or objectives, despite this aspect of social media being a focus of early press reporting and public awareness." 2, SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 ELECTION, 7 (2019), https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

301. *See, e.g.*, Dean Dechlaro, *Curbing Disinformation: How much should Social Media Companies do?*, ROLL CALL (Oct. 29, 2019 7:00 AM), https://www.rollcall.com/news/congress/curbing-disinformation-much-social-media-companies; Renee DiResta & Mike Godwin, *The Seven Step Program for Fighting Disinformation*, JUST SECURITY (Feb. 28, 2019), https://www.justsecurity.org/62718/step-program-fighting-disinformation/.

302. Kaplan, *supra* note 290.

303. Nir Grinberg et al., *Fake News on Twitter During the 2016 U.S. Presidential Election*, 363 SCIENCE 374 (2019).

304. Casey Newton, *People Older than 65 Share the Most Fake News, New Study Finds*, THE VERGE (Jan. 9, 2019, 2:00 PM). https://www.theverge.com/2019/1/9/18174631/old-people-fake-news-facebook-share-nyu-princeton.

305. Recent articles have pointed to the example of Finland, which, in 2014, launched in a multi-pronged education and awareness campaign for its 5.5 million citizens, aimed at countering the Russian propaganda

the 2020 Presidential election season is providing fodder for the debate over content moderation and transparency in advertising on social media platforms. Facebook continues to battle consumer privacy class action litigation over its sharing of detailed personal information of millions of users with political consulting firm Cambridge Analytica – perhaps the starkest example to date of personal data profiles being used to manipulate political opinion.[306] As 2019 was drawing to a close, Democratic political candidate Elizabeth Warren posted a deliberately false ad on Facebook to illustrate the ways in which Facebook's advertising policies allow political campaigns to direct micro-targeted advertising at potential voters.[307]

As the U.S. considers what legislative, regulatory, or other steps might fit within the American legal framework, the ways in which the government of Russia has leveraged detailed personal profiles as a means to direct political advertising and political influence campaigns not only provides evidence of the current risks, but suggests the ways in which individual data profiles could be used even more aggressively by foreign and domestic actors to influence social issues, election outcomes, and other area of public opinion and individual action in the future.

X. A PROPOSAL FOR NEW CONGRESSIONAL COMMITTEES ON DATA-DRIVEN TECHNOLOGIES

Conventional wisdom suggests that law and policy will always struggle to keep pace with changes in technology. That a task may be difficult, however, shouldn't dissuade lawmakers from considering meaningful approaches to tackling the problems of balancing the privacy and autonomy interests of individuals with the importance of economic growth and corporate innovation. Not to mention the national security need for appropriately constrained government investigation and surveillance.

---

messages that have been directed against Finland since that country gained its independence nearly a century ago. The lessons address how to identify bots on Twitter, how to spot deep fake videos, and how to spot slanted news coverage and identify an outlet's or an article's biases, all as part of an initiative to counter Russian information warfare that attempted to stoke divisions over issues such as immigration, the European Union, and NATO. These measures alone may not be enough to counter the ways in which our individual information is being used to manipulate our views. But it appears to be having positive effect, both in maintaining civil discourse in Finland and in preserving free and fair elections there. Countries across Europe and from other parts of the world are looking to Finland's experience to create critical thinking and public education programs of their own. As part of a larger toolkit, Finland's lessons could contribute in important ways to countering the negative effects of platforms that know the details about us entirely too well. *See, e.g.*, Reid Standish, *Why is Finland Able to Fend off Putin's Information War?*, FOREIGN POLICY (Mar. 1, 2017), https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/.

306. *In re* Facebook Biometric Information Privacy Litig., No. 3:15-cv-03747-JD (N.D. Cal. Aug. 17, 2015). *See also* Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

307. Cecilia Kang & Thomas Kaplan, *Warren Dares Facebook with Intentionally False Political Ad*, N.Y. TIMES (Oct. 12, 2019), https://www.nytimes.com/2019/10/12/technology/elizabeth-warren-facebook-ad.html.

Just as has been the case historically, Congress continues to establish new committees when circumstances warrant. And although many issues in Congress are so fraught with partisan tension that bipartisan or bicameral agreement can be difficult to achieve, American legal, policy, and political discourse on data privacy and the uses and impact of personal data have reached a tipping point in which bipartisan, bicameral action may be possible. In the current Congress, committees in both the Democrat-controlled House and Republican-controlled Senate have held hearings on proposals for federal data privacy legislation. Members of Congress in both parties have called for investigations of whether and to what extent anti-trust laws should be employed to rein in the growth and power of major technology platform providers such as Google, Facebook, and Amazon.[308]

Privacy advocacy groups are paying more attention to the ways in which personal data can be used to exploit workers in the gig economy,[309] and California's recently enacted California Consumer Privacy Act contains provisions which will, beginning in January, 2021, grant employees new and expanded rights with respect to personal data collected by their employers.[310] With attention from advocacy groups as well as state legislatures, members of Congress may well find themselves facing questions from constituents about whether and how these issues might be addressed at the federal level. Members of both parties have reason to be concerned about the extent to which the imbalance between European and American approaches to individual data privacy could impede transnational data transfer and, with it, American economic growth. Additionally, members of both parties have raised significant concerns about election security and voter manipulation. Several bipartisan bills have been proposed in both chambers that would address issues including transparency around micro-targeted political advertising, this is advertising which inherently depends on detailed personal profiles of the targeted individuals.[311]

The recently established House Committee on the Climate Crisis is one example of a recently formed Committee designed to address a particular problem set.[312]

---

308. *See, e.g.*, Steve Lohr, *New Google and Facebook Inquiries Show Big Tech Scrutiny is Rare Bipartisan Act*, N.Y. TIMES (Sept. 6, 2019), https://www.nytimes.com/2019/09/06/technology/attorney-generals-tech-antitrust-investigation.html.

309. As noted by one advocacy group, "the so-called "gig economy" has brought to light employers' increasing ability and willingness to monitor employee performance, efficiency, and overall on-the-job conduct. Workplace surveillance of gig economy workers often happens without employees' awareness or consent. This is especially evident in the app-based gig economy, where apps act both as an important tool for employees to do their job, while also being a means for employers to conduct active surveillance of their workers." *Case Study: The Gig Economy and Exploitation*, PRIVACY INT'L., https://privacyinternational.org/case-study/751/case-study-gig-economy-and-exploitation.

310. CAL. CIV. CODE §§ 1798.100-.199 (Deering 2018).

311. *See, e.g.* Election Security Act of 2019, S. 1540, 116th Cong. (2019). *See also* Press Release, Office of Senator James Lankford, Bill Adds DHS'S Cybersecurity and Infrastructure Agency to Election Assistance Commission's Committee that Creates Cybersecurity Guidelines (May 14, 2019).

312. H.R. Res. 6, 116th Cong. § 104(f)(2)(A)(2019) (enacted).

That Committee, however, is not well-postured for meaningful success. The Committee is comprised of 15 members selected by House leadership; but there is no requirement, or even any recommendation, that those members overlap in any way with membership of other key committees with jurisdiction over related subject matters.[313] The committee has no legislative jurisdiction and no authority to take legislative action.[314] Although the committee's role is purely investigative, it has no subpoena power – it can only recommend subpoenas to other committees with authority to issue them[315] – and it has no authority to hire its own staff.[316] This reality severely diminishes the likelihood that the committee will have the services of professional staff with expertise in matters relating to climate change available to it. The framework and structure of the House committee on climate change is precisely the opposite of what is required to make meaningful progress on a complex and far-reaching topic within a short time. It is un-resourced, unempowered, and unable to propose legislative changes; it is, therefore, also unlikely to deliver significant progress is helping Congress or the American people determine how best to move forward on potential approaches to addressing climate change. That doesn't make the Committee on climate change irrelevant. It may well conduct hearings that provide meaningful information to the public and may well produce reports that provide useful insights and recommendations. But the committee is in no position to drive change.

The Church and Pike Committees, by contrast, were established with resources, subpoena power, intentionally overlapping jurisdiction and expertise, a specific mandate to propose and to review legislation, and authority to hire a professional, non-partisan staff. These critically important substantive, procedural, and administrative tools were backstopped by a widely shared bipartisan concern over the scope of intelligence-gathering activities, particularly as those activities involved collecting and retaining information of and about U.S. citizens. Although members of the two major parties then, and now, would draw the line in a slightly different place on the balance between individual privacy and security, members of both parties, and the bipartisan membership of the intelligence committees over the ensuing years, have unanimously agreed on the importance on both of these values that are in tension with each other. They agree on the importance of preserving both security and privacy.

Thanks in part to the enduring legacy of the Church and Pike Committees, the intelligence activities of the U.S. government are subject to regular, rigorous oversight. They are conducted in a fashion that is arguably more transparent than any other nation in the world, and with levels of transparency that have generally increased over time. The successor House and Senate Intelligence Committees

313. *Id.*

314. *Id.*

315. *Id.* § 104(f)(2)(B).

316. *Id.* § 104(f)(4)(A).

have continued to oversee intelligence community activities, to propose new legislation and to review legislative proposals from other committees. They serve as an important mechanism in ensuring continued effectiveness of national security programs as well as continued review of the measures in place to protect the privacy of individuals. The framework established by Church and Pike, while imperfect,[317] has continued to serve vital interests and important functions.

A similar bipartisan national sentiment is emerging on the importance of tackling the diversity of issues presented by data-driven technologies. This support makes this an appropriate, indeed an auspicious, time to establish bipartisan Select Committees on Data Driven Technologies ("DDT") in the House and Senate that are empowered to conduct meaningful, wide-ranging, and well-informed investigations, and to propose comprehensive, nuanced, and sensible legislation. The key features of such DDT Committees should include the following:

1) Limited membership, to ensure meaningful participation and discussion. Notionally, this could number 15 members in the Senate Committee and 21 members in the House committee, evenly split between majority and minority, with the tie-breaking member being of the majority party.

2) Intentional overlap of membership with the key committees in each chamber already responsible for other aspects of legislative and investigative activity relating to data privacy and data-driven technologies. These would include the Senate Committees on Banking, Commerce, Homeland Security, Intelligence, Judiciary. On the House side, these would include the Committees on Education and Labor, Energy and Commerce, Financial Services, Homeland Security, Intelligence, Judiciary, and Space, Science and Technology. Representation should include one majority and one minority member from each committee with formally designated overlap.

317. The effectiveness of the intelligence committees, like other Congressional committees, depends in part on the temperament and conduct of their leadership, and on a willingness to adhere to important norms that are not inherently enforceable via other means. This dependence was abundantly clear through the conduct of the House and Senate Intelligence Committees during the 115th Congress. During that term, which included calendar years 2016-2017, the House Intelligence Committee was chaired by Rep. Devin Nunes, with Ranking Member Rep. Adam Schiff. The Senate Intelligence Committee was chaired by Sen. Richard Burr, with Vice Chair Mark Warner. Both committees conducted investigations into Russian government interference in the 2016 U.S. Presidential elections. The House intelligence committee's investigation was largely viewed as compromised by the highly partisan loyalties of HPSCI Chair Nunes, who officially recused himself from the investigation during the course of the 115th Congress. *See* Emmarie Huetteman, *Devin Nunes to Step Aside from House Investigation*, N.Y. TIMES (Apr. 6, 2017), https://www.nytimes.com/2017/04/06/us/politics/devin-nunes-house-intelligence-committee-russia.html. In contrast, the SSCI received consistently high marks for its bipartisan approach to this politically fraught investigation, under the leadership of two senators – Burr and Warner – who throughout the course of the investigation maintained a joint public commitment to bipartisan fact-finding and to the integrity of the Senate Intelligence Committee as an institution. *See* Olivia Gavis, *Richard Burr on the Senate Intelligence Committee's Russia Investigation, 2 Years on*, CBS NEWS (Feb. 7, 2019, 5:51 AM), https://www.cbsnews.com/news/richard-burr-on-senate-intelligence-committees-russia-investigation-2-years-on/on/ (last updated on Feb. 7, 2019, 12:53 PM).

3) Subpoena power for witnesses and documents, vested in both the Chair and Ranking Member or Chair and Vice Chair, depending on terminology adopted by the DDT Committees.

4) Budget allocation for a permanent, professional staff commensurate with the scope of the DDT Committees' activities. In addition to the usual skill sets of lawyers and legislative and policy aides, the Committees should incorporate a Senior Technology Advisor or similar role, and should include a number of staff positions specifically designated to be filled by individuals with critically-needed technology skills, including data science, computer science, cryptomathematics, and similar fields.

5) Authority to propose new legislation and to review the legislative proposals of other committees when those proposals include subject matter that falls within the new DDT Committees' jurisdiction. These new DDT Committees should have a defined scope and task that includes a two-year timeline to investigate issues relating to data science, privacy, and technology, to make legislative proposals on those issues, and to make recommendations on whether there is a need to institutionalize their efforts as standing committees in future sessions of Congress.

CONCLUSION

The Church Committee report included the following items in its list of chief concerns about government surveillance activities: 1) "the number of people affected;" 2) "too much information is collected for too long," 3) "covert action and … the use of illegal or improper means," 4) "ignoring the law," 5) "deficiencies in accountability and control," 6) the "adverse impact" on individuals of "improper" use of data, and 7) "cost and value" of those activities.[318] When abstracted from the specific context of 1970s oversight of government surveillance activities to the larger landscape of modern data-intensive technologies, it becomes clear that these seven areas of concern could just as easily describe society's' growing sense of unease with the ways in which information is collected and used by private sector actors in the modern economy.

Members and committees in both houses of Congress are making laudable efforts to explore the many privacy, antitrust, labor and employment, and other issues being raised by data-intensive technologies. But few of these efforts are supported by dedicated professional staff with a background in the relevant technologies. Few of them are being carried out with legislative resources – staff, committee prominence or influence, budgets – that are commensurate to the challenges posed by this large and growing sector of the American economy. And none are taking place within committees that are fully empowered with the full scope of jurisdictional reach that could maximize their effectiveness. The creation of new, fully empowered Select Committees on Data-Driven Technologies that are

318. See *supra*, Section IV.

resourced, staffed, and granted sufficient jurisdiction to hold wide-ranging hearings and propose cross-functional legislation could have a significant positive impact on Congress's ability to keep pace with the challenges raised by these rapidly evolving technologies.

Although it is unlikely that such new committees would be incorporated into the legislative framework during the 116th Congress, this is a move that Congressional leadership could and should consider. If not adopted during the 116th Congress, the proposal should be further reviewed and refined for consideration and potential adoption by incoming leadership of the 117th Congress in January 2021.