ARTICLES

CONGRESSIONAL SURVEILLANCE

AARON R. COOPER*

In recent years, Congress has increasingly used electronic surveillance in high-profile investigations. Reactions to what this Article calls "congressional surveillance" indicate a deep unease among both legal scholars and the broader public about the nature of Congress's surveillance authority and its normative implications. Despite our ongoing preoccupation with government surveillance, congressional surveillance remains largely unexplored. There is virtually no discussion of how congressional surveillance is treated under key statutory and Fourth Amendment constraints; no consideration of the process or political limits of congressional surveillance; and little scrutiny of congressional surveillance as a tool within the separation of powers.

This Article fills that gap by presenting the first scholarly treatment of congressional surveillance. It argues that to address congressional surveillance, we must first understand its hybrid features of both government surveillance and congressional political power.

Specifically, the Article makes two contributions. First, the Article argues that congressional surveillance operates under fundamentally different constraints than traditional government surveillance. Congressional processes and politics ("process limits") constrain congressional surveillance more than established

* Adjunct Professor of Law, *Georgetown University Law Center*. Special Counsel, Jenner & Block LLP. Thanks to Josh Chafetz, Jen Daskal, Gus Hurwitz, Katie Keith, Alan Rozenshtein, Jodi Short, Christopher Slobogin, and the University of Nebraska Law and Tech Virtual Workshop for helpful comments on drafts and to Greg Klass, Julie O'Sullivan, and Robin West for advice. Thanks also to the 2020 Minnesota Cybersecurity Law and Policy Scholars Conference for providing the impetus for this project. The views expressed herein are my own, and do not necessarily reflect the views of Jenner & Block LLP.

statutory and Fourth Amendment mechanisms ("external limits") or the inherent constraints of congressional authority ("internal limits").

Second, this Article argues that congressional surveillance is justified as an essential practice within the separation of powers. It offers legitimate benefits to Congress in inter-branch information disputes with the executive and in carrying out basic digital governance. The Article also argues that the Supreme Court's decision in Trump v. Mazars USA, LLP *mistakes a privacy concern that congressional surveillance poses as a threat to the separation of powers. At the same time, this Article rejects the traditional law enforcement approach to protecting individual privacy through judicial gatekeeping. Instead, the Article argues that the treatment of congressional surveillance must account for individual privacy interests while preserving Congress's ability to assert itself as a co-equal branch—not the* Mazars *approach, and not a law enforcement approach, but something different.*

TABLE OF CONTENTS

INTRODUCTION

Congress surveils. In 2017, the Senate Select Committee on Intelligence (SSCI) obtained data pertaining to millions of social media interactions from major American service providers—including Facebook, Instagram, Google, YouTube, and Twitter—for its investigation into Russian election interference.[1] It did so without using any legal process, instead persuading providers to share the data voluntarily.[2] In December 2019, as part of the first impeachment inquiry into President Donald Trump, the House Permanent Select Committee on Intelligence (HPSCI) subpoenaed phone records from multiple telecommunications providers.[3] The records revealed that President Trump's personal attorney, Rudy Giuliani, and Congressman Devin Nunes, among others, had been in contact with an alleged fraudster and key player in orchestrating a deal with Ukraine to investigate the President's political rival.[4]

The responses were telling. Experts debated whether Congress's access to social media data violated the Stored Communications Act[5] (SCA), the law that governs disclosures of user information by communications service providers.[6] Outrage over the disclosed phone

---

1. S. SELECT COMM. ON INTEL., 116TH CONG., RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION, VOL. 2: RUSSIA'S USE OF SOCIAL MEDIA, S. REP. NO. 116-290, at 3–4, 43–58 (Comm. Print 2020) [hereinafter SSCI REPORT].

2. *Id.* at 3–4.

3. *See* H. PERMANENT SELECT COMM. ON INTEL., 116TH CONG., THE TRUMP-UKRAINE IMPEACHMENT INQUIRY REPORT, H.R. REP. NO. 116–335, at 44–46 & 153 n.49 (Comm. Print 2019) [hereinafter HPSCI REPORT]. In total, the House issued six subpoenas to three providers: Verizon, AT&T, and CSC Holdings. Scott Wong & Juliegrace Brufke, *Controversy on Phone Records Intensifies amid Impeachment*, HILL (Dec. 10, 2019, 6:00 AM), https://thehill.com/homenews/house/473769-controversy-on-phone-records-intensifies-amid-impeachment [https://perma.cc/6GK4-9RKT].

4. *See* Wong & Brufke, *supra* note 3 (describing subpoena controversy).

5. 18 U.S.C. §§ 2701–2713.

6. Ryan Goodman, *Is It Legal for Facebook to Disclose Its Russian Election Ads?*, NEWSWEEK (Oct. 30, 2017, 10:21 AM), https://www.newsweek.com/it-legal-facebook-disclose-its-russian-ads-696139 [https://perma.cc/A6CC-SSLZ] (conveying views of legal experts on "whether and to what extent, if any, a federal law—the Stored

records graced *The Wall Street Journal*,[7] *Fox News*,[8] and *The New York Times*.[9] Controversy ensued, triggering "perhaps the most heated debate about phone metadata in Washington since former government contractor Edward Snowden's 2013 revelations of the intelligence community's broad collection of such records."[10]

These reactions indicate a deep unease among both legal scholars and the broader public about Congress's use of electronic surveillance. Congress has long enjoyed the authority to compel evidence from third parties, using its Article I subpoena power to inquire into private and criminal conduct.[11] But only recently have congressional committees leveraged their subpoena authority to collect electronic evidence, like call records and social media data, and applied forensic and analytical tools to understand their import.[12] With this shift,

---

Communications Act—restricts Facebook's ability to share the content of Russian ads and related information with Congress and the public").

7. *See, e.g.*, Kimberley A. Strassel, *Adam Schiff's Surveillance State: An FCC Official Calls Him Out for Obtaining Call Records Without Judicial Review*, WALL ST. J. (Mar. 12, 2020, 7:09 PM), https://www.wsj.com/articles/adam-schiffs-surveillance-state-11584050541 [https://perma.cc/C49G-RXC5] (referring to the action as an "abuse of power"); John Solomon, *Schiff Threatens Press Freedom: When the Surveillance State Exposes a Journalist and His Sources, There's an Instant Chilling Effect*, WALL ST. J. (Dec. 9, 2019, 7:28 PM) https://www.wsj.com/articles/schiff-threatens-press-freedom-11575937690 [https://perma.cc/FBV4-W95L] (expressing anger that Rep. Schiff does not find it reasonable for Congress to have similar guardrails as the executive branch to protect privacy).

8. *See, e.g.*, Julia Musto, *Nunes Rips Schiff Over Subpoena of Phone Records: 'I Actually Have Some Civil Rights Here, Too,'* FOX NEWS (Dec. 5, 2019), https://www.foxnews.com/media/devin-nunes-adam-schiff-phone-record-impeachment-subpoena [https://perma.cc/AAX8-C72G] (discussing the subpoena of one's phone records as an "infraction of his 'civil rights'").

9. Marc Ambinder, *Did Schiff Poke a Hole in the First Amendment?*, N.Y. TIMES (Dec. 16, 2019), https://www.nytimes.com/2019/12/16/opinion/first-amendment-impeachment.html [https://perma.cc/FX4Z-RG2S] (discussing the "disturbed" feeling of hearing Rep. Schiff's actions).

10. *See, e.g.*, Cat Zakrzewski, *The Technology 202: Phone Records from AT&T and Verizon Obtained in Impeachment Inquiry Spark Controversy*, WASH. POST (Dec. 9, 2019, 9:14 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/12/06/the-technology-202-phone-records-from-at-t-and-verizon-obtained-in-impeachment-inquiry-spark-controversy/5de93d5188e0fa652bbbdc1e.

11. *See infra* Section I.B.1.

12. For instance, as part of its impeachment investigation, House investigators used digital forensic tools to extract information from the cell phone of a witness, Lev Parnas, who had been in communication with individuals in President Trump's circle. *See* Joseph Cox, *House Democrats Used Cellebrite to Publish Lev Parnas iPhone Messages*, VICE (Jan. 15, 2020, 11:01 AM), https://www.vice.com/en_us/article/wxednb/house-

Congress has begun to embrace the surveillance power of the digital world, engaging in what this Article calls *congressional surveillance*.

To be sure, plenty of ink has been spilled on the topic of government surveillance more broadly. Court decisions instruct the government to "get a warrant" when it seeks to obtain the contents of emails or cell phone location data.[13] Congress has enacted comprehensive regimes to regulate law enforcement and national security surveillance, including the Electronic Communications Privacy Act of 1986[14] (ECPA) and the Foreign Intelligence Surveillance Act of 1978[15] (FISA).[16] And the academic literature offers a rich discussion of the ways in which these statutes,[17] the Fourth Amendment,[18] procedural

---

democrats-used-cellebrite-lev-parnas-apple-iphone-messages [https://perma.cc/9BHY-N4S5]. The SSCI leveraged analytical work on its social media data by third-party researchers. SSCI REPORT, *supra* note 1, at 3 n.3. (collecting notes and text messages from an associate of Rudy Giuliani).

13. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2222–23 (2018) (holding that the Fourth Amendment requires a warrant for the government to compel a provider to disclose seven days of cell-site location information); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the Fourth Amendment requires a warrant for the government to compel a provider to disclose the contents of emails).

14. Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2523).

15. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1862).

16. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1266 (2004).

17. *See, e.g.*, Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 376–78 (2014) (recommending updates to the Electronic Communications Privacy Act to reflect developments in technology); Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 485–86 (2013) (examining privacy statutes with attention to law enforcement exceptions and their relationship to the Fourth Amendment); Solove, *supra* note 16, at 1266 (examining the failures of electronic surveillance law and proposing that "[w]arrants supported by probable cause should be required for most uses of electronic surveillance").

18. *See generally* Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 809 (2016) (arguing that, as applied to the Internet of Things, Fourth Amendment "effect[s]" should be understood using a theory of "digital curtilage"); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1007 (2010) (presenting a general theory of how the Fourth Amendment applies to Internet communications); Peter P. Swire, Katz *Is Dead. Long Live* Katz., 102 MICH. L. REV. 904, 905 (2004) (arguing that Fourth

mechanisms,[19] and even private sector entities[20] interact to facilitate or constrain government surveillance.

However, congressional surveillance exposes a core and unstated assumption in how we think about government surveillance: namely, that it is a creature of *executive* authority.[21] As a result, scholars have tended to overlook the surveillance authorities of *Congress*.[22] Indeed, despite our ongoing preoccupation with the surveillance state, Congress's ability to use its broad subpoena authority as a form of

---

Amendment jurisprudence plays a useful role in the context of electronic surveillance and other high-tech searches and seizures).

19. *See, e.g.*, Andrew Manuel Crespo, *Systemic Facts: Toward Institutional Awareness in Criminal Courts*, 129 HARV. L. REV. 2049, 2050, 2052, 2054 (2016) (arguing that courts can have a supervisory role over police surveillance); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 95 (2016) (arguing that "the concrete rules governing panvasive techniques should be viewed through the entirely different prism of administrative law"); Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1827 (2015) (arguing that all forms of policing, including surveillance, "should be legislatively authorized, subject to public rulemaking, or adopted and evaluated through some alternative process that permits democratic input"); John Rappaport, *Second-Order Regulation of Law Enforcement*, 103 CALIF. L. REV. 205, 205 (2015) (arguing that the U.S. Supreme Court should adopt the "second-order regulation," a type of "regulatory design choice" that "enunciate[s] constitutional values and create[s] incentives for political policy makers to write the conduct rules"); Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. BRIEF 1, 1–2 (2011) (contending that magistrate judges may impose ex ante restrictions on how police search computer hard drives).

20. *See, e.g.*, Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 667 (2019) (analyzing the role of U.S. technology companies "in the digital ecosystem and in international affairs"); Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 99 (2018) (offering a framework to understand how U.S. technology companies "constrain the surveillance executive" (emphasis omitted)); Ian Samuel, *The New Writs of Assistance*, 86 FORDHAM L. REV. 2873, 2873–74 (2018) (arguing that government surveillance should be restrained through reforms of technology company data practices).

21. *See, e.g.*, William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 13, 74 (2000) (discussing the necessity for—and intentional limits on—executive surveillance).

22. It is not unusual for Congress to be the forgotten branch, and even when attention is paid, the treatment has elided important aspects of Congress's role. *See, e.g.*, JOSH CHAFETZ, CONGRESS'S CONSTITUTION: LEGISLATIVE AUTHORITY AND THE SEPARATION OF POWERS 2 (2017) (arguing that "the exclusively legislation-focused view of Congress is far too narrow"); NEAL DEVINS & KEITH E. WHITTINGTON, *Introduction* to CONGRESS AND THE CONSTITUTION 2 (Neal Devins & Keith E. Whittington eds., 2005) ("The study of the Constitution has largely been defined within the academy as the study of constitutional law as produced by the courts," in which "Congress is a target" and "not a producer").

electronic surveillance remains largely unexplored and, judging from public reaction, widely misunderstood.[23] Scholars have seldom considered how congressional surveillance fares under key privacy regimes, like the SCA or the Fourth Amendment's warrant requirement. We have no record of the procedural or political constraints on congressional surveillance. And there is little scrutiny of congressional surveillance as a tool within the separation of powers.[24]

The Supreme Court began to address these issues in *Trump v. Mazars USA, LLP*,[25] its recent decision that cast a skeptical eye on the House of Representatives' subpoenas for financial information to President Trump's banks and accountants. The Court warned that, absent new limits, "Congress could declare open season on the President's information held by schools, archives, internet service providers, email clients, and financial institutions."[26] Motivated by this fear, it imposed a new balancing test—not one based on privacy considerations—rather, one that reflects the "weighty concerns regarding the separation of powers" when congressional surveillance targets the President.[27] Yet the Court's narrow decision reflects the profound uncertainty around congressional surveillance, both descriptive and normative.

This Article presents the first scholarly treatment of congressional surveillance. It argues that to address congressional surveillance, we must first understand its hybrid features of both government surveillance *and* congressional political power. In doing so, it makes two contributions.

First, this Article makes the descriptive claim that congressional surveillance exhibits fundamentally different characteristics than traditional government surveillance. In doing so, it presents a conceptual framework to understand congressional surveillance as it differs from other, more common forms of government surveillance.

---

23. Candice Norwood, *How Do Congressional Subpoenas Work?*, PBS (Oct. 10, 2019, 10:02 AM), https://www.pbs.org/newshour/politics/how-do-congressional-subpoenas-work [https://perma.cc/P4V4-Z3VK] (explaining the basics of congressional subpoenas in response to audience questions).

24. When Congress's role in surveillance is considered, it is usually in the context of oversight of surveillance by the executive branch. *See* Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 646–47 (2017) (discussing judicial and scholarly opinions arguing that the legislative branch should be responsible for surveillance oversight).

25. 140 S. Ct. 2019 (2020).

26. *Id.* at 2035.

27. *Id.* at 2035–36.

This framework, which borrows from a "useful typology" of congressional limits,[28] pairs the legal basis and tools of congressional surveillance—described in Part I—with its corresponding *external*, *internal*, and *process* limits—described in Part II.[29] In this framework, *external limits* are sources of positive law, such as statutes and the Bill of Rights, that constrain an otherwise valid exercise of government surveillance. *Internal limits* represent the inherent constraints of government surveillance authority, taken on its own terms. *Process limits* control the way in which the government can, or cannot, choose to exercise its surveillance authority.

This framework shows that congressional surveillance is constrained more by congressional process and politics (the *process limits*) than established statutory and Fourth Amendment mechanisms (the *external limits*) or the inherent constraints of its authority (the *internal limits*). The *external limits* on government surveillance, in the form of legislation and the Fourth Amendment, apply to Congress in profoundly different ways. Congressional surveillance is largely outside the reach of key provisions of the SCA, and it is also not subject to the Fourth Amendment's warrant requirement.[30] The *internal limits* on congressional surveillance are highly permissive, granting Congress significant discretion in what it chooses to investigate, how it uses its subpoena power, and the disclosure of the information it acquires. Finally, congressional surveillance exhibits distinctive *process limits*, a feature of Congress's design as a self-regulated, transparent, and publicly accountable political body.

---

28. Richard Primus, *The Limits of Enumeration*, 124 YALE L.J. 576, 578–79 (2014) (citing LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 297 (2d ed. 1988)) (describing the three kinds of limits of congressional power: internal limits, external limits, and process limits).

29. A system-level framework such as this helps to overcome "cultural translation" barriers between surveillance practices of different branches of government. *See* Lynn M. LoPucki, *The Systems Approach to Law*, 82 CORNELL L. REV. 479, 514 (1997) (explaining that those who observe events in one cultural context find it difficult to describe the event to someone in another cultural context). It is also a pre-condition to offering normative arguments about how a surveillance system *should* be designed. *See id.* at 503.

30. Specifically, as discussed in Section II.A.1, the SCA does not regulate at all congressional access to metadata and other non-content information; in fact, it may even permit a congressional subpoena for the contents of a communication. Meanwhile, as discussed in Section II.A.2, the Fourth Amendment considers congressional legal process under a reasonableness regime, without imposing a warrant requirement for constructive searches.

This is not quite a Congress unbound, but close.[31] Taken as a whole, this picture raises thorny questions about the institutional design of Congress's surveillance authorities: "not simply *what* the limits on communications surveillance should be, but *who* should set them."[32] After all, Congress is not a law enforcement agency, so it should not necessarily be regulated as one.

Second, this Article argues that congressional surveillance represents an important tool in the separation of powers and can be normatively justified on those grounds.[33] As Part III argues, congressional surveillance is not "mere" surveillance, but is a way for Congress to compete for authority within the separation of powers, a form of what Josh Chafetz terms "constitutional politics."[34] Congressional surveillance can serve as a potent tool for Congress to counter the White House's ever-increasing invocations of executive privilege in inter-branch information disputes.[35] And it can empower Congress to engage in digital governance rather than ceding that responsibility to technology companies.

---

31. *Cf.* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 15–16 (2010) (arguing that major "constraints on the executive" do not arise from law or from the separation-of-powers framework); Ashley Deeks, *Facebook Unbound?*, 105 VA. L. REV. ONLINE 1, 2 (2019) (exploring "why it has proven difficult for Congress and the courts (and the Executive) to weave a set of legal constraints around technology companies").

32. Patricia L. Bellia, *Designing Surveillance Law*, 43 ARIZ. ST. L.J. 293, 295 (2011) (emphasis added).

33. In this way, the Article also contributes to separation of powers literature, addressing how Congress can more effectively influence and counter the executive branch and compete for political power. Josh Chafetz, for instance, has argued that Congress can leverage its traditional powers more effectively, contending that "political power is largely endogenous to politics." CHAFETZ, *supra* note 22, at 17 (emphasis omitted). Rebecca Ingber has illustrated how Congress influences the executive's foreign policy apparatus through tools of "congressional administration." Rebecca Ingber, *Congressional Administration of Foreign Affairs*, 106 VA. L. REV. 395, 400 (2020); *see also* Saikrishna Bangalore Prakash, *Congress as Elephant*, 104 VA. L. REV. 797, 799, 802 (2018) (arguing that Congress "play[s] multiple, vital roles" and "has the tools to dominate its interbranch rivals"); Jack M. Beermann, *Congressional Administration*, 43 SAN DIEGO L. REV. 61, 64 (2006) (surveying ways in which Congress is involved in "the day to day administration of the law").

34. CHAFETZ, *supra* note 22, at 16.

35. Numerous articles have interrogated the contours of executive privilege. *See, e.g.*, Jonathan David Shaub, *The Executive's Privilege*, 70 DUKE L.J. 1, 2 (2020) (offering a limited theory of executive privilege); Patricia M. Wald & Jonathan R. Siegel, *The D.C. Circuit and the Struggle for Control of Presidential Information*, 90 GEO. L.J. 737, 737–38 (2002) (exploring models for resolution of disputes over presidential information).

In making this argument, this Article challenges the framing in *Mazars*, where the Supreme Court treated this new dynamic as a separation of powers *concern* rather than a separation of powers *benefit*.[36] This Article contends that *Mazars* muddles the background privacy threat posed by congressional surveillance with a distinct separation of powers issue.[37] In doing so, the *Mazars* decision places a finger on the separation of powers scale in favor of the President and the courts without addressing the broader privacy implications. In a sense, then, *Mazars* gets it backwards. Instead, as this Article concludes, the treatment of congressional surveillance must account for case-by-case privacy interests while preserving Congress's ability to assert itself as a co-equal branch.[38] A richer understanding of congressional surveillance is needed to make that possible, and this Article takes a first step in that direction.

I. CONGRESS'S SURVEILLANCE SHIFT

Surveillance is pervasive these days,[39] and Congress is no longer an exception. The legislative branch, like its executive counterpart, has

---

36. Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2033–34 (2020).

37. *Cf.* Daphna Renan, *The President's Two Bodies*, 120 COLUM. L. REV. 1119, 1123 (2020) (arguing that "'the President' is an amalgamation of the individual president and the institutional presidency," which underlies an inherent tension in public law).

38. I should flag here what this Article is *not* about. It is not about private sector surveillance, although it assumes that private companies have data that Congress wants. *See, e.g.*, Mariano-Florentino Cuéllar & Aziz Z. Huq, *Economies of Surveillance*, 133 HARV. L. REV. 1280, 1286 (2020) (reviewing SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) and discussing the pros and cons of private surveillance); Jack M. Balkin, *The First Amendment in the Second Gilded Age*, 66 BUFFALO L. REV. 979, 984 (2018) (suggesting that private "digital media companies are *information fiduciaries* who have duties of care and loyalty toward their end-users"). Second, this Article is not about the First or Fifth Amendments, although these are important areas for continuing study. *See, e.g.*, Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 114 (2007) (arguing that "First Amendment activities are implicated by a wide array of law enforcement data-gathering activities"). Third, this Article is not about the political machinations of individual members of Congress. For simplicity, it treats Congress, each chamber, and the committees as units, but does not delve into the inter-personal dynamics of individual members or party structures, also candidates for future work.

39. For a few recent works on the growth of surveillance, both public and private, *see, e.g.*, Cuéllar & Huq, *supra* note 38, at 1280 (exploring surveillance economies); Bruce Schneier, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD ch. 6 (2015) (examining the consolidation of government and corporate surveillance); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV.

begun to exert its authority as a surveillance power, gaining access to private, digitized information and harnessing technology to understand it. Although Congress has long wielded investigative powers, congressional surveillance is different. Why? Because society's shift to digital communication expands the type and magnitude of information that Congress can access, much as it has in the law enforcement and national security space. As this Part argues, Congress's access to electronic information meaningfully alters the authority it possesses, implicating privacy and civil liberties concerns, even as its authority remains stubbornly congressional in nature.

A. Congressional ***Surveillance***

Congressional inquiries into private information are not, on their own, a new phenomenon.[40] Two examples of recent vintage stand out. Beginning in 1953, Senator Joseph McCarthy infamously led the Senate Permanent Subcommittee on Investigations into the proverbial witch-hunt of communist "sympathizers." Meanwhile, in the House of Representatives, the Un-American Activities Committee interrogated witnesses on their political activities and personal connections. Of those investigated, 135 were criminally prosecuted for refusing to testify.[41] During the Watergate investigations, Congress pursued President Nixon's personal tape recordings of conversations with his former counsel, John Dean.[42] These events and others illustrate

---

1934, 1935–36 (2013) (exploring the various ways that government surveillance harms society).

40. Congress investigated non-governmental activity and punished non-members "[a]lmost from the beginning." CHAFETZ, *supra* note 22, at 172; *see also* JAMES HAMILTON, THE POWER TO PROBE 102 (1976) (observing that Congress has conducted investigations of criminal activity "since its nascence"). More recently, Congress has investigated "mob violence and organized crime," *In re* Application of U.S. Senate Permanent Subcomm. on Investigations, 655 F.2d 1232, 1233 (D.C. Cir. 1981), and "sex trafficking, on the Internet," Senate Permanent Subcomm. v. Ferrer, 199 F. Supp. 3d 125, 128 (D.D.C. 2016), *vacated as moot*, 856 F.3d 1080 (D.C. Cir. 2017).

41. *See* Geoffrey R. Stone, *Free Speech in the Age of McCarthy: A Cautionary Tale*, 93 CALIF. L. REV. 1387, 1389, 1400 (2005). During the McCarthy era, some witnesses refused to give testimony on their associates and litigated the ensuing convictions for criminal contempt. The Court addressed the issue not as a matter of privacy or free association, but rather as a matter of due process, on the grounds that the committee's authorizing resolution had not given sufficient notice of the nature of the inquiry. *See infra*, Section II.B.

42. Senate Select Comm. on Presidential Campaign Activities v. Nixon, 498 F.2d 725, 731 (D.C. Cir. 1974) (upholding Nixon's claim of executive privilege as to the

Congress's long-standing interest in private information, at times to excess.[43]

Congressional *surveillance* is different from these historical examples, for at least two reasons. *First*, routine digital activities create new kinds of information that do not exist elsewhere, such as metadata, online search histories, behavioral profiles, detailed activity tracking, and records of precise location information, among others.[44] In particular, "the Internet of Things offers new surveillance possibilities that do not involve any physical intrusion into the object."[45] This is an especially important change for an entity like Congress that, as I will describe, does not have a recognized physical search or seizure authority.

Second, the growth of service providers and cloud computing have facilitated the transfer of user control over personal data to third-party entities.[46] Emails and communications records, for instance, are no longer stored on a laptop or other local device, but instead in the cloud, where they are maintained by a service provider like Google,

---

Senate subpoena because the Senate committee had not shown tapes were "demonstrably critical" when they had been produced already to the House).

43. The Supreme Court in *United States v. Watkins* recounted an 1835 inquiry by a committee of the British House of Commons into "the Orange Institutions," a "political-religious organization, vehemently Protestant in religion and strongly in favor of the growth of the British Empire." 354 U.S. 178, 191 (1957). At a certain point, the committee demanded that an official of the Orange Institutions produce all records of the organization. *Id.* The official was imprisoned after he "refused to turn over a letter-book" that contained, in addition to official records, other "records of private communications with respect to Orangeism." *Id.*

44. *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 93–97 (2019) (describing the "behavioral surplus" and epistemic harvest of "surveillance capitalism"); SCHNEIER, *supra* note 39, at 17 ("Data is the exhaust of the information age."). Even the Supreme Court has referred to this information as "an entirely different species of business record." Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018). That does not mean that the law lacks the capacity to address it, however. *See* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 756 (2016) (arguing that "[d]ata [i]s [n]ot [s]o [d]ifferent" from other intangible assets for jurisdictional purposes).

45. Ferguson, *supra* note 18, at 810; *see also* Richards, *supra* note 39, at 1940 (discussing the shift in connectivity from primarily computers and smartphones to an "Internet of Things" comprised of connected appliances, homes, and power grids).

46. *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1689 (2018) (describing cloud computing as being internet-based rather than locating resources on a personal computer and highlighting the accompanying legal issues).

Microsoft, or Amazon, sometimes in the United States, sometimes elsewhere, or even in many places at once.[47]

Together, these developments mean that Congress, like its executive branch counterpart, has access to *more* and *different* information. And because third parties often control the data, Congress can access that data in a different *way*, without requiring users' involvement, or even their knowledge.[48]

Imagine a present-day McCarthy who, instead of parading witnesses in and out for testimony on their personal and political affiliations,[49] procured their location information, the URLs of the websites they visited, and their emails and text messages. Or, instead of a physical recording of the Watergate tapes, consider a President who prefers to record voice memos on an iPhone and saves them to an iCloud account.[50] Consider if, rather than seeking the information from the White House, Congress could simply obtain the recordings from Apple, along with information about when, how and by whom it was uploaded.

Even more recent events just scratch the surface. The HPSCI's subpoena of phone records from third-party providers during its 2019 impeachment inquiry into President Donald Trump is not the first time Congress has obtained phone records.[51] But, consider extensions

---

47. *See, e.g.*, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 200 (2d Cir. 2016) (explaining that Microsoft produced data it stored in the United States but declined to produce customer data it stored in Ireland), *vacated and remanded by* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018); *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 709 (E.D. Pa. 2017) (holding that the government can require Google to produce customer data stored outside of the United States).

48. As an obvious consequence, the data subject may no longer assert a Fifth Amendment right against production of the data—an objection otherwise available if the subject still possesses the records. *See, e.g.*, Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 825–26 (2005) (describing the effect of the "Information Age" on the use of third-party subpoenas).

49. *See, e.g.*, Barsky v. United States, 167 F.2d 241, 252 (D.C. Cir. 1948) (upholding constitutionality of inquiry into individual's political beliefs and party membership against a First Amendment challenge); Lawson v. United States, 176 F.2d 49, 50–52 (D.C. Cir. 1949) (same).

50. *See, e.g.*, *VEEP: Testimony* (HBO television broadcast June 7, 2015).

51. For instance, during the Whitewater investigation, Republicans obtained and disclosed Hillary Clinton's phone records, claiming that they were evidence of obstruction. *See* David Maraniss, *The Hearings End Much as They Began*, WASH. POST (June 19, 1996), https://www.washingtonpost.com/wp-srv/politics/special/whitewater/stories/wwtr960619.htm [https://perma.cc/JAY7-DVL3].

of a phone records request, such as a subpoena for detailed GPS or cell site location information from the same entities. Or consider the digital messaging equivalent of toll records—the address information in emails or direct messages that can provide the who, what, and when of private electronic communications. The SSCI's acquisition of provider data to track the Russian Internet Research Agency's (IRA) influence campaign was not all that different, involving a bulk data set containing millions of social media interactions.[52]

What these examples suggest is that congressional surveillance is not business as usual for Congress; rather, it is an old habit on steroids. Congress's acquisition of this digital information, just like any other government entity, should raise different concerns than run-of-the-mill subpoenas.[53] It is no surprise, then, that disclosures to Congress have prompted broad and complex questions as to the legality of voluntary information sharing by providers, as well as Congress's ability to compel the production of such information. But, as I turn to next, Congress is not using new *authorities*. Rather, Congress is directing its traditional authorities towards new *information* and new *entities*, which reflect the emergence of a new *congressional surveillance*.

B. ***Congressional*** *Surveillance*

At the same time, congressional surveillance remains stubbornly *congressional* in both purpose and scope. It supports Congress's Article I responsibilities of legislation, oversight, and impeachment. Congressional surveillance is limited to information already in possession of a third party, or what we can call "derivative surveillance." This is a stark contrast to executive branch surveillance, which is driven by Article II imperatives of law enforcement and national security and involves proactive surveillance authorities like real-time network surveillance and actual (as opposed to constructive) searches and seizures.[54]

This Section addresses the two primary ways that Congress can conduct surveillance. First, Congress can exercise its subpoena authority to obtain user data from providers such as phone companies,

---

52. SSCI REPORT, *supra* note 1, at 7, 77.

53. Cuéllar & Huq, *supra* note 38, at 1330 (arguing that "the state still presents a distinctive kind of risk to human agency and well-being in a surveillance economy").

54. *See, e.g.*, United States v. Abu-Jihaad, 630 F.3d 102, 113–15 (2nd Cir. 2010) (detailing methods the government used to obtain evidence against Abu-Jihaad, including a wiretap).

social media platforms, messaging services, and similar entities. Second, Congress can ask providers to cooperate by disclosing user data, a mechanism that can become quite powerful in light of Congress's ability to regulate—and therefore incentivize—the technology industry.

1. Surveillance subpoenas

Government surveillance is often associated with the types of intrusive, far-reaching, and covert activities of remote searches, pen registers, wiretaps, and bulk data collection.[55] In comparison, congressional surveillance is almost rudimentary. Congress's compulsory authority is limited to its subpoena power,[56] and even then, only as necessary to fulfill its Article I roles. Congress's authority to issue subpoenas is not written directly into the Constitution, but instead derives from historical custom[57] and a common-sense understanding that a legislative and oversight body is only as effective as its ability to secure the necessary information to discharge its constitutional responsibilities.[58]

The Supreme Court articulated the reason for an implied compulsory power in *McGrain v. Daugherty*,[59] which tested the enforceability of a testimonial subpoena against the former attorney

---

55. *See* Bellia, *supra* note 32, at 290–302 (describing the evolving scope of communications surveillance); Adrienne LaFrance, *Same Surveillance State, Different War: How Government Justification for Mass Surveillance During the War on Drugs Turned into Rationalization for Spying on Citizens in the War on Terror*, ATLANTIC (Apr. 8, 2015), https://www.theatlantic.com/technology/archive/2015/04/same-surveillance-state-different-war/389988 [https://perma.cc/52TG-58EY] (tracing "a continuum" between the "pre-9/11" Drug Enforcement Administration (DEA) "War on Drugs" surveillance program and "post-9/11 War on Terror" national security surveillance programs).

56. As in other contexts, a congressional subpoena for the production of things is called a *subpoena duces tecum* and a subpoena for witness testimony is called a *subpoena ad testificandum*.

57. The legislature's power to compel predates recognition by U.S. courts. *See, e.g.*, Josh Chafetz, *Congress's Constitution*, 160 U. PA. L. REV. 715, 735 (2012) (acknowledging the long-standing understanding that Congress can hold nonmembers in contempt); William P. Marshall, *The Limits on Congress's Authority to Investigate the President*, 2004 U. ILL. L. REV. 781, 785–88 (2004) (providing a historical overview of Congress's investigatory powers).

58. *See generally* CHAFETZ, *supra* note 22, at 153–80 (tracing the historical development of the contempt power from the inception of Parliament to contemporary U.S. practice).

59. 273 U.S. 135 (1927).

general.[60] The Court acknowledged that Congress's power to compel testimony—if it existed—must be implicit because no constitutional provision explicitly grants either house the ability to "make investigations and exact testimony."[61] The Court therefore considered "whether this power is so far incidental to the legislative function as to be implied," and concluded that it is.[62]

The Court's reasoning highlighted two central considerations. First, the Court acknowledged that Congress "cannot legislate wisely or effectively" without access to relevant information held by others.[63] Second, the Court acknowledged that Congress cannot rely on voluntary cooperation to acquire relevant information because "mere requests for such information often are unavailing, and also that information which is volunteered is not always accurate or complete"; therefore, "some means of compulsion are essential."[64] Together, these considerations undergird what is now a commonly accepted practice of compulsory congressional power.[65]

As a result, Congress has long enjoyed the power to issue subpoenas and enforce them,[66] using this power to compel witnesses to sit for hearings and depositions and to produce documents and records.[67]

---

60. *Id.* at 150–52.

61. *Id.* at 161.

62. *Id.* at 161, 174.

63. *Id.* at 175. It naturally follows that Congress lacks that authority if no possible legislation can be had—an internal limit that I address in Section II.B.

64. *McGrain*, 273 U.S. at 175.

65. The Court placed this authority in historical context:

> All this was true before and when the Constitution was framed and adopted. In that period the power of inquiry—with enforcing process—was regarded and employed as a necessary and appropriate attribute of the power to legislate—indeed, was treated as inhering in it. Thus, there is ample warrant for thinking, as we do, that the constitutional provisions which commit the legislative function to the two houses are intended to include this attribute to the end that the function may be effectively exercised.

Id.

66. The ways in which Congress enforces subpoenas has evolved over time, from inherent contempt (an implied power) to criminal contempt and civil enforcement (both statutory mechanisms). *See* TODD GARVEY, CONG. RSCH. SERV., RL34097, CONGRESS'S CONTEMPT POWER AND THE ENFORCEMENT OF CONGRESSIONAL SUBPOENAS: LAW, HISTORY, PRACTICE, AND PROCEDURE 17 (2017) (tracing the historical transition of Congress's enforcement methods).

67. *See* MORTON ROSENBERG & TODD B. TATELMAN, CONG. RSCH. SERV., RL34097, CONGRESS'S CONTEMPT POWER: LAW, HISTORY, PRACTICE, AND PROCEDURE 1 (2007) (explaining that the "contempt power has generally been employed only in instances

But in important ways, *McGrain*'s depiction of Congress is incomplete—it does not speak to a variety of core congressional functions, such as confirmation of appointees, appropriations, oversight, and impeachment.[68] For example, when the HPSCI compelled the production of phone records from AT&T, Verizon, and CSC Holdings, it did so as part of an *impeachment* inquiry, not for a legislative purpose.[69] *McGrain*'s limited depiction of congressional power suggests that a compulsory authority is a necessary adjunct.[70]

A subpoena can be a powerful tool, especially in light of the changes described above. When a third party observes and records every-day activities, the theoretical reach of a congressional subpoena is meaningfully expanded by the business practices of private sector entities. As Orin Kerr has argued, changes in storage technology and user behavior have made stored data more prevalent and revealing than even real-time communications.[71] But even so, subpoenas are limited in their authority, which necessarily limits congressional surveillance. A subpoena can direct a person to produce a file from that person's computer, but it cannot authorize the government's

---

of refusals of witnesses to appear before committees, to respond to questions, or to produce documents" for the last seventy years).

68. *See, e.g.*, CHAFETZ, *supra* note 22, at 2 (decrying the legislation-oriented understanding of Congress's role).

69. *See* HPSCI REPORT, *supra* note 3, at 7–10, 45 (describing phone records obtained by three congressional committees in support of House impeachment inquiry); *see also* Sonne et al., *Phone Logs in Impeachment Report Renew Concern About Security of Trump Communications*, WASH. POST (Dec. 6, 2019, 11:59 AM), https://www.washingtonpost.com/world/national-security/phone-logs-in-impeachment-report-renew-concern-about-security-of-trump-communications/2019/12/05/2066fbf4-16fe-11ea-8406-df3c54b3253e_story.html [https://perma.cc/JEH2-RSDW] (noting that phone records obtained as part of House impeachment inquiry had no indication that calls were encrypted or otherwise protected from foreign surveillance).

70. Courts often characterize impeachment as a more compelling justification of congressional power than other roles. *See, e.g.*, Senate Select Comm. on Presidential Campaign Activities v. Nixon, 498 F.2d 725, 732 (D.C. Cir. 1974) (noting that impeachment investigations in the House have "an express constitutional source" that sets them apart from Congress's general oversight or legislative powers). Even while dissenting in *Mazars*, Justice Thomas stressed that he viewed the subpoena power in furtherance of impeachment as categorically different from other congressional functions. 140 S. Ct. 2019, 2037–47 (2020) (Thomas, J., dissenting).

71. *See, e.g.*, Kerr, *supra* note 17, at 393 ("When everything is stored, stored access begins to reveal the same level of detail as real-time access . . . . If anything, stored access is even more revealing and invasive. Real-time surveillance is cabined by time.").

seizure of that computer to obtain the same file without consent.[72] Likewise, a subpoena cannot be used to wiretap a private phone call, but it can be used to obtain a pre-existing recording of the call[73] or records indicating that the call occurred.[74]

One could certainly argue that more intrusive investigative techniques, such as physical searches or wiretaps, would be effective aids to congressional investigations.[75] That Congress is not understood to possess this authority reinforces the notion that it does not act in a purely law enforcement capacity.[76] Congress has never formally asserted—nor has any court ever held—that Article I grants it the authority to enter and search private property for information. Likewise, Congress cannot break down doors to execute an arrest, seize a cell phone from a criminal suspect, or wiretap a member of an international criminal gang such as Mara Salvatrucha (MS-13), like the Federal Bureau of Investigations (FBI) or Drug Enforcement Administration (DEA). Rather, Congress exercises *derivative* surveillance authorities, such that it can compel the production of information that others possess, but no more.

---

72. *See, e.g.*, Donovan v. Lone Steer, Inc., 464 U.S. 408, 413–14 (1984) (distinguishing entry into public lobby of motel-restaurant to serve subpoena, which did not authorize either entry or inspection of premises, from administrative searches of non-public work areas that require a warrant). Section II.A.2 discusses situations where the Fourth Amendment nevertheless treats a subpoena as a constructive search.

73. *See* Nixon v. Sirica, 487 F.2d 700, 736–37 (D.C. Cir. 1973) (MacKinnon, J., concurring in the judgment) (per curiam) (resolving that "every public document, paper, or record, or copy thereof" relating to an issue under Congress's power to investigate "is subject to the call or inspection of the Senate").

74. *Id.*

75. For example, it is said that "the public . . . has a right to every man's evidence," United States v. Bryan, 339 U.S. 323, 331–32 (1950), and "[c]ongressional subpoenas seek information in aid of the power to legislate for the entire nation while judicial subpoenas seek information in aid of the power to adjudicate controversies between individual litigants in a single civil or criminal case," Nixon v. Sirica, 487 F.2d at 737 (MacKinnon, J., concurring in part). Indeed, there is nothing that limits search or seizure authorities to criminal law enforcement or national security because they are available in administrative contexts as well. *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523, 538–39 (1967).

76. I distinguish here between Congress's Article I functions and the authority it has codified for the Capitol Police, which may perform certain law enforcement activities under specified conditions. *See* 2 U.S.C. § 1961. The Sergeant-at-Arms exercises the same law enforcement authorities as the Capitol Police, *see id.* § 6617 (Senate); *id.* § 5605 (House), with the additional responsibility in the House to "execute the commands of the House and all processes issued by authority thereof, directed to him by the Speaker." *Id.* § 5604.

2. Cooperative surveillance

Much of what Congress does is an exercise of soft power.[77] Congress exercises its soft power to obtain *cooperative surveillance*—that is, voluntary disclosures of private, digital information.[78] Congress's reliance on cooperation is not unusual in this context. Congress holds countless hearings every year, receives briefings, conducts interviews, and takes depositions, many of which it conducts on a voluntary basis. This is because witnesses believe the costs of ignoring Congress are too high or (and perhaps in addition) they want to convey a particular opinion or version of events.[79]

Voluntary disclosures of user data are a rare occurrence in the post-Snowden world.[80] But in 2017, the SSCI obtained a voluntary production of data from social media providers as part of its investigation into Russian election interference.[81] The data included the following:

> [m]etadata and content associated with 81 Facebook Pages, including approximately *61,500 unique Facebook organic posts* and 3,393 paid advertisements; [s]imilar information from nearly *116,000 Instagram posts* across 133 Instagram accounts; [m]etadata and content of approximately *10.4 million tweets* across 3,841 Twitter accounts, as well as unique account information; and, [a]pproximately *1,100 YouTube videos* (43 hours of video) across 17 account channels.[82]

---

77. CHAFETZ, *supra* note 22, at 3. In Chafetz's framework, which borrows from international relations, "soft power" is "the ability to get what you want through attraction rather than coercion or payments." *Id.* (quoting Joseph S. Nye, Jr., *Soft Power and American Foreign Policy*, 119 POL. SCI. Q. 255, 256 (2004)); *see also* Jacob E. Gersen & Eric A. Posner, *Soft Law: Lessons from Congressional Practice*, 61 STAN. L. REV. 573, 577, 594 (2008) (outlining the variety of ways Congress utilizes soft law to impact the behavior of others when more formal legal mechanisms are less desirable).

78. *Cf.* Gersen & Posner, *supra* note 77 at 590–91 (describing situations in which industries took voluntary steps in response to congressional resolutions).

79. A third possibility might be a sense of civic obligation. *See, e.g.*, Watkins v. United States, 354 U.S. 178, 187 (1957) ("It is unquestionably the duty of all citizens to cooperate with the Congress in its efforts to obtain the facts needed for intelligent legislative action.").

80. The law enforcement context includes cooperative surveillance as well, such as under the Stored Communications Act—where a provider may, but is not compelled to, disclose data to government authorities within an emergency disclosure. *See* 18 U.S.C. § 2702(b)(8).

81. *See supra* note 1 and accompanying text.

82. SSCI REPORT, *supra* note 1, at 77 (emphasis added).

This was not merely data reflecting public or commercial activity, such as advertisements, but also account metadata.[83] Putting aside the fact that these were fake accounts controlled for purposes of deception, the data included the types of information that government authorities normally obtain only pursuant to statutorily authorized legal processes, such as a court order under the SCA.[84] Yet here, the SSCI obtained this data without any legal process at all. According to press accounts, the providers were initially hesitant to make these disclosures.[85] But, as the SSCI held hearings and public attitudes began to shift, the providers reconsidered; that is, the "politics of the situation" changed."[86]

In theory, voluntary cooperation is divorced from the assertion of Congress's coercive power: the provider may choose whether to furnish the desired information. In reality, the companies holding this information are subject to legislation and oversight, which create

---

83. Researchers who were granted access to the data by the Committee published an analysis demonstrating just how deeply the data could be mined. *See* Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency* 3, 16–20, 66 (NEW KNOWLEDGE), https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf [https://perma.cc/DZ5R-JNJ9] (analyzing substantial data sets of social media metadata and Russia's Internet Research Agency's "influence operations targeting American citizens from 2014 through 2017"); Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* 3, 7–8, 10–11 (COMPUTATIONAL PROPAGANDA RSCH. PROJECT), https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/The-IRA-Social-Media-and-Political-Polarization.pdf [https://perma.cc/C4SE-KL9T] (investigating the ways in which Russia "exploited" social media platforms' metadata to "impact US users"). Twitter later released the data publicly. *See* Vijaya Gadde & Yoel Roth, *Enabling Further Research of Information Operations on Twitter*, TWITTER: CO. BLOG (Oct. 17, 2018), https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html [https://perma.cc/C2WM-5TSJ].

84. 18 U.S.C. § 2703(d) (outlining the requirements for a court order requesting disclosure of information).

85. *See, e.g.*, Ryan Lucas, *The Next Big Focus in the Russia Investigations: Social Media*, WBUR (Sept. 22, 2017), https://www.wbur.org/npr/552726960/the-next-big-focus-in-the-russia-investigations-social-media [https://perma.cc/G9VA-RKB7] ("Facebook has briefed congressional investigators about the ads, and it has provided the ad content to Justice Department special counsel Robert Mueller. Lawmakers have complained, however, that the company had refused to hand over copies of the documents to the congressional committees.").

86. Goodman, *supra* note 6 (explaining that there is typically a "significant political upside for a social media company to . . . say 'No' to the government").

strong incentives to comply with congressional demands.[87] Witness testimony and document production inescapably occur in the shadow of Congress's compulsory power and the surrounding political dynamic.

Nevertheless, voluntary disclosures are no less significant from a surveillance standpoint than compelled disclosures. Regardless of whether Congress obtains location data, contact lists, or private messages pursuant to a subpoena or voluntarily, Congress has the same authority to use that information, with the same implications for privacy. Congress's ability to obtain voluntary cooperation is a powerful surveillance tool, no less so than its compulsory counterpart.

II. THE LIMITS OF CONGRESSIONAL SURVEILLANCE

Having delineated the basic contours of congressional surveillance and its authorities, this Part turns to understanding its limits. I assess three kinds of limits on congressional power: external limits, internal limits, and process limits.[88] By applying this framework, rather than focusing on a specific limit in isolation, I allow for a more complete understanding of congressional surveillance. In particular, I discuss how congressional surveillance is and is not constrained, provide essential context for where it diverges in meaningful ways from other forms of government surveillance, and establish a basis for normative considerations identified here and explored further in Part III. This framework shows that congressional surveillance is constrained more by congressional process and politics (the process limits) than established statutory and Fourth Amendment mechanisms (the external limits) or the inherent constraints of its authority (the internal limits).

---

87. Some scholars have even gone so far as to conclude that political pressure coupled with responsive actions make the social media companies effectively state actors. Jed Rubenfeld, *Are Facebook and Google State Actors?*, LAWFARE (Nov. 4, 2019, 8:20 AM), https://www.lawfareblog.com/are-facebook-and-google-state-actors [https://perma.cc/AV4Z-H8UB] (arguing that social media companies like Facebook and Google are functionally equivalent to state actors when they "block 'objectionable' content"). Doctrinal questions aside, the relationship between legislators and the entities over which they legislate merits consideration. *See, e.g.*, Abbey Stemler, *Platform Advocacy and the Threat to Deliberative Democracy*, 78 MD. L. REV. 105, 107–09 (2018) (examining the potential influence that social media and internet-based platforms have on their users to influence legislation).

88. Primus, *supra* note 28, at 578–79 (defining the boundaries of Congress's powers in terms of "process," "external," and "internal limits").

A. External Surveillance Limits

External limits are the affirmative prohibitions that constrain an otherwise valid exercise of government authority,[89] and they provide the core constraints on government surveillance. Statutes like ECPA and FISA, along with the Fourth Amendment,[90] are the main vehicles through which the law regulates executive surveillance.[91] Given these limitations, one might reasonably conclude that Congress's ability to engage in digital surveillance is equally constrained by these sources of law. But that is not entirely true. While our experience with executive surveillance creates certain expectations about how these sources of law limit government surveillance, they do not apply equally to Congress. Instead, Congress falls entirely outside the reach of some key surveillance limits, occupying an effectively unregulated space.

This is evident in two ways. First, the SCA, a part of ECPA that regulates access to stored data, imposes no barriers on congressional access to non-content information and may even, I argue, permit Congress to obtain the contents of communications with a subpoena rather than a warrant. Second, the Fourth Amendment treats congressional subpoenas under the rubric of a constructive search for which the Supreme Court has imposed a "reasonableness" standard, not a strict warrant requirement. Thus, neither source of law provides the same type of limits for the legislative branch as it does for the executive branch; to the contrary, they are surprisingly lenient.

1. ECPA and statutory privacy

ECPA—and its various components[92]—is one of the primary non-constitutional vehicles for protecting digital privacy and regulating

89. *Id.* at 578.

90. U.S. CONST. amend. IV.

91. *See, e.g.*, Solove, *supra* note 16, at 1266 (observing that "ECPA and FISA are the heart of electronic surveillance law"); Slobogin, *supra* note 19, at 96 (noting "the understandable belief that the Fourth Amendment, as a practical matter, has preempted the field of police regulation"). For example, an authoritative Department of Justice manual focuses on these two sources of law for the collection of electronic evidence in criminal investigations, to the tune of approximately 200 of its 210 substantive pages. *See* COMPUT. CRIME & INTELL. PROP. SECTION, CRIM. DIV. DEP'T OF JUST., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS *passim* (2009) https:// www. justice.gov/ sites/ default/ files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf [https://perma.cc/ P22M-Y6FS]; *see also* U.S. DEP'T OF JUST., JUSTICE MANUAL § 9-7.010 (2020).

92. ECPA incorporated the SCA as Title II, but ECPA separately included amendments to the Wiretap Act and created the Pen Register and Trap and Trace

government surveillance of digital communications and computer networks.[93] While ECPA's expansive framework covers live intercepts under the Wiretap Act[94] and pen registers under the Pen/Trap Statute,[95] this Section focuses on the SCA, which purports to regulate the stored data the HPSCI obtained in its 2019 impeachment inquiry and the account information the SSCI obtained in its Russia investigation.[96]

The SCA is a complicated statute,[97] but this discussion addresses two narrow questions: first, should the SCA's framework for compelled disclosures also regulate congressional surveillance and, second, should the SCA's constraints on provider disclosures be understood to limit congressional authority? My arguments on both issues advance notions of congressional exceptionalism—specifically, that Congress treats its investigative demands differently than the executive branch and should not be presumed to curtail its own power except in limited and unambiguous circumstances.

a. Statutory exceptionalism

Congress jealously guards its investigative authorities, which it views as core to its Article I powers, and it legislates accordingly. That is, Congress regulates itself differently than it does the other branches, such that it avoids imposing categorical limits on its own authority, and when it does, it uses special language to do so. This exceptionalism is

---

Statute. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848; Stored Communications Act, 18 U.S.C. §§ 2701–2713.

93. Orin Kerr has described in detail the intent behind the various provisions of ECPA, many of which are not intuitive. *See generally* Kerr, *supra* note 17 (noting that ECPA grants internet users a set of statutory privacy rights that limit the government's power to access a person's communications and records); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) [hereinafter Kerr, *User's Guide*] (explaining the basic structure and text of ECPA, including its distinctions and dichotomies, so that others may better understand how it works).

94. 18 U.S.C. § 2511.

95. 18 U.S.C. §§ 3121–3127.

96. As discussed in Part I, a subpoena does not extend to live interception. That said, the repeated production of stored electronic communications is effectively the same as a real-time interception. *See* Kerr, *User's Guide*, *supra* note 93, at 1232 (noting a First Circuit decision holding that emails copied mid-transmission were governed by the SCA because they were "copied when in 'storage,'" even if only for a split second).

97. The SCA is a notoriously difficult statute to parse, even among challenging statutes. *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (generously observing the SCA's "lack of clarity").

key to understanding how the SCA and similar privacy-protecting statutory schemes treat Congress.

First, outside of Title 2 of the U.S. Code,[98] Congress has tended to avoid self-regulating legislation that implicates its constitutional functions.[99] Instead, chamber and committee rules and procedures serve as its preferred form of self-governance.[100] As to its investigative powers, Congress has sought to *increase* its statutory right to information over time, not limit it.[101] For example, it has passed laws giving federal courts subject matter jurisdiction over civil litigation to enforce Senate subpoenas,[102] granting whistleblowers rights to report malfeasance to Congress[103] and requiring federal agencies to affirmatively provide information to Congress.[104] From a balance of powers perspective, this makes sense. After all, limiting Congress's access to information through legislation would effectively grant to the judicial and executive branches oversight power over the legislature. Congress is especially sensitive to these transfers of power when they concern its essential fact-finding functions.[105]

---

98. *See, e.g.*, 2 U.S.C. § 2(a) (providing the time and manner in which representatives are reapportioned).

99. *See* Harold H. Bruff, *That the Laws Shall Bind Equally on All: Congressional and Executive Roles in Applying Laws to Congress*, 48 ARK. L. REV. 105, 123–39 (1995) (describing congressional self-regulation in core and "quasi-constitutional functions"). The exceptions consist primarily of statutes that regulate "proprietary functions," public interactions with Congress such as lobbying laws, and criminal prohibitions. *Id.* at 140; *see also* Congressional Accountability Act of 1995, Pub. L. No. 104-1, 109 Stat. 3 (applying to Congress substantive provisions of laws governing employment, anti-discrimination, and health and safety).

100. For instance, Congress runs its own ethics investigations and has the power to discipline its members. *See, e.g.*, Theresa A. Gabaldon, *The Self-Regulation of Congressional Ethics: Substance and Structure*, 48 ADMIN. L. REV. 39, 40–41, 67–68 (discussing options for improved congressional self-regulation in ethics).

101. These statutes include mechanisms to incentivize production of information, including false statements and contempt laws, as well as mechanisms to increase oversight authorities with respect to the executive branch. *See generally* CHRISTOPHER M. DAVIS ET AL., CONG. RSCH. SERV., RL30240, CONGRESSIONAL OVERSIGHT MANUAL 5–9 (2020) (summarizing laws that "augment and safeguard Congress's authority, mandate, and resources").

102. 28 U.S.C. § 1365.

103. Whistleblower Protection Act of 1989, Pub. L. No. 101–12, 103 Stat. 16.

104. *See, e.g.*, 50 U.S.C. § 3901 (requiring intelligence committees to be "fully and currently informed of the intelligence activities").

105. For example, as Josh Chafetz argues, enactment of the statutory contempt crime did not displace Congress's inherent contempt authority. As he puts it, "[e]ven assuming, arguendo, that Congress *could* have surrendered this power entirely, there

Second, a disclosure to Congress as part of an Article I investigation serves a different purpose than disclosure in other contexts. As a result, courts have treated disclosures to Congress as special, requiring a clear statutory statement of any intent to curtail Congress's authority.[106] For example, in one line of cases involving congressional access to trade secrets, the D.C. Circuit repeatedly held that the Federal Trade Commission (FTC) *could* disclose confidential information in response to Congress's investigative demands, including through subpoenas, even though it was statutorily *prohibited* from disclosing that same information to the public.[107] The court's reasoning was motivated, in part, by the sense that "the judiciary must refrain from slowing or otherwise interfering with the legitimate investigatory functions of Congress."[108] As the committee argued at the time, a different decision would have had a "severe and widespread" impact on Congress's fact-finding abilities: approximately 150 statutory provisions prohibited disclosure of information obtained by a federal agency without specifically referencing disclosures to Congress.[109]

---

is no evidence that it intended to deliver its ability to enforce its demands for information wholly into the hands of executive prosecutorial discretion." Chafetz, *supra* note 57, at 736.

106. *See, e.g.*, McKinley v. Bd. of Governors of the Fed. Rsrv. Sys., 849 F. Supp. 2d 47, 60 (D.D.C. 2012) ("Disclosures to Congress are not official disclosures within the meaning of FOIA . . . .").

107. Exxon Corp. v. Fed. Trade Comm'n, 589 F.2d 582, 585–89 (D.C. Cir. 1978); *see* Fed. Trade Comm'n v. Owens-Corning Fiberglas Corp., 626 F.2d 966, 968 (D.C. Cir. 1980) (assuming that the FTC and any congressional committees with which it shares subpoenaed documents will handle that confidential information appropriately); Ashland Oil, Inc. v. Fed. Trade Comm'n, 548 F.2d 977, 979 (D.C. Cir. 1976) (per curiam) (holding that it was permissible for the FTC to disclose confidential information to Congress). At the time, section 6 of the Federal Trade Commission Act empowered the FTC "[t]o make public from time to time such portions of the information obtained by it hereunder, except trade secrets and names of customers, as it shall deem expedient in the public interest." *See* Federal Trade Commission Act of 1914, Pub. L. No. 63-203, § 6(f), 38 Stat. 717, 721. Congress has since amended the provision. *See* Federal Trade Commission Improvements Act of 1980, Pub. L. No. 96-252, § 3, 94 Stat. 374, 374–75 (codified at 15 U.S.C. § 46(f)).

108. Owens-Corning Fiberglas Corp., 626 F.2d at 970.

109. H.R. SUBCOMM. ON OVERSIGHT AND INVESTIGATIONS OF THE COMM. ON INTERSTATE AND FOREIGN COM., 95TH CONG., THE *ASHLAND* LITIGATION: A CASE STUDY IN JUDICIAL DELAY OF A CONGRESSIONAL INVESTIGATION 10 (Comm. Print 1977) (discussing the significance of the threat posed by the *Ashland* litigation to Congress's power to seek out information in support of its legitimate legislative function).

A similar dynamic has played out under the Right to Financial Privacy Act of 1978[110] (RFPA), on which Congress specifically modeled the SCA.[111] The RFPA prohibits disclosures of customer records by financial institutions to a "[g]overnment authority," except in limited circumstances, which do not include a congressional subpoena.[112] In *Trump v. Deutsche Bank AG*[113] (a companion case to the *Mazars* litigation), President Trump argued that, because of this language, the RFPA barred the House from compelling the bank to produce his financial information.[114] The Second Circuit disagreed.[115] The court focused on the plain text and limited definition of "[g]overnment authority," which under the RFPA means an "agency or department of the United States,"[116] and concluded that the statute did not restrict the House's subpoena.[117]

In other statutes, Congress has unequivocally expressed that its own powers should be limited. A classic example is congressional access to

110. 12 U.S.C. §§ 3401–3423.

111. S. REP. NO. 99-541, at 3 (1986) ("[The SCA] is modeled after the Right to Financial Privacy Act, 12 U.S.C. 3401 et seq. to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs.").

112. 12 U.S.C. § 3402. The exceptions include customer consent, or when required in response to an administrative subpoena, search warrant, judicial subpoena, or formal written request from a government authority. *Id.*

113. 943 F.3d 627 (2d Cir. 2019), *vacated*, 140 S. Ct. 2019 (2020).

114. *Id.* at 641.

115. *Id.* at 645.

116. 12 U.S.C. § 3401(3). The terms "department" and "agency" of the United States are defined by 18 U.S.C. § 6, which I discuss further in the context of the SCA in Section II.B.1.ii, below. The Second Circuit panel also observed that a draft bill presented by the Departments of Justice and the Treasury had proposed including Congress within the definition of "government authority," but this was not adopted in the final language. *See Deutsche Bank*, 943 F.3d at 642 n.25 (discussing *Electronic Funds Transfer and Financial Privacy: Hearing on S. 2096, S. 2293, and S. 1460 Before the Subcomm. on Fin. Insts. of the S. Comm. on Banking, Hous., & Urb. Affs.*, 95th Cong. 397 (1978)).

117. *Deutsche Bank*, 943 F.3d at 641–45. The plaintiffs did not appeal this aspect of the Second Circuit's decision to the Supreme Court, and it remains undisturbed by *Mazars*.

tax returns.[118] In § 6103 of the Internal Revenue Code,[119] Congress established a "[g]eneral rule" that prohibits the disclosure of federal tax return information, absent express statutory authorization.[120] The Internal Revenue Code then provides a series of exceptions to the general rule, each pertaining to a particular class of government officials and interested parties and for specifically identified purposes.[121] Here, the statute explicitly authorizes disclosure of tax return information only upon written request by the chair of the House Committee on Ways and Means, the chair of the Senate Finance Committee, or the chair of the Joint Committee on Taxation.[122] Other committees seeking such information must follow the procedures outlined in the statute.[123]

These statutes show that when Congress wants to limit its own authority, it does so explicitly. There are no implied abdications of Congress's authority, and a general limitation on disclosure does not create a corresponding limit on Congress. This backdrop provides necessary context for my argument that the SCA does not restrict Congress's subpoena authority, which I turn to next.

b. Congress's SCA

Congress enacted the SCA as part of ECPA's broader effort to enhance digital privacy in both stored and live communications. A specific focus of the SCA, like ECPA more generally, was to address perceived gaps in how the Fourth Amendment applied to electronic

118. *See generally* Amandeep S. Grewal, *The President's Tax Returns*, 27 GEO. MASON L. REV. 439, 441–48 (2020) (examining legislative history relating to tax privacy); George K. Yin, *Preventing Congressional Violations of Taxpayer Privacy*, 69 TAX LAW. 103, 120 (2015) ("Congress was wary of giving itself authority over, or access to, the confidential information, apparently out of concern that doing so might unduly jeopardize the privacy rights of taxpayers.").

119. 26 U.S.C. § 6103.

120. *Id.* § 6103(a).

121. *Id.* § 6103(c)–(o).

122. *Id.* § 6103(f)(1).

123. *Id.* § 6103(f)(3). Several recent articles have discussed Congress's use of these provisions in relation to taxpayer privacy, addressing both congressional access to and subsequent disclosure of tax return information. *See, e.g.*, Grewal, *supra* note 118, at 446, 456 (discussing the balance between granting congressional access to tax return information and protecting taxpayer privacy); Yin, *supra* note 118, at 105–06 (arguing that the House Ways and Means Committee violated the law in 2014 when it voted to publicly release tax return information for fifty-one individuals).

communications held by third parties.[124] The SCA regulates access to user data through two mechanisms.[125] First, in § 2702, the SCA limits a provider's[126] *voluntary* disclosures of user data.[127] Second, in § 2703, the SCA provides a mechanism by which a "governmental entity" may *compel* the production of data from a provider.[128]

Some experts have assumed that the SCA extends to Congress, just as it does to other government entities.[129] Under this view, the statute does not permit voluntary disclosures to Congress under § 2702 in the absence of an applicable exception, and Congress may not compel the production of information under § 2703 unless it follows the established framework.[130] The following discussion addresses that view, offering a competing interpretation that would leave Congress's subpoena authority untouched under the SCA as to non-content data, and possibly even as to content data.

---

124. *See* Kerr, *User's Guide*, *supra* note 93, at 1209–12 (discussing why the Fourth Amendment's privacy protections may not apply to electronic communications). Kerr highlights three reasons for this gap. First, it is not clear the Fourth Amendment applies because there remains uncertainty over whether internet users have a reasonable expectation of privacy in information they send and receive. Second, its application is complicated by rules allowing grand jury subpoenas compelling Internet service providers ("ISPs") to disclose information. Finally, most ISPs are private actors, and thus, the Fourth Amendment does not apply to any searches they may undertake. *Id.*

125. *See id.* at 1223 (summarizing the two mechanisms in a table). Kerr has written extensively on the SCA and ECPA. *See generally* Kerr, *supra* note 17, at 378–90 (discussing the history and structure of ECPA). However, Kerr's focus has been on law enforcement access; he does not discuss how Congress fits into the statutory scheme.

126. For ease of reference, I call these "service providers" or "providers," although the statute divides them into two groups: providers of electronic communications service ("ECS") and providers of remote computing service ("RCS"). *See* 18 U.S.C. § 2702(a)(1)–(2). Generally, providers of ECS are akin to email and messaging services, whereas providers of RCS are more like cloud storage or web hosting providers, but the SCA does not cover data held by other entities, such as businesses that just happen to have an online presence. *See* Kerr, *User's Guide*, *supra* note 93, at 1216–17. The difference between providers of ECS and RCS is not relevant here.

127. 18 U.S.C. § 2702.

128. *Id.* § 2703.

129. Goodman, *supra* note 6 (canvassing experts on the SCA's effect on Facebook's ability to share the content of Russian ads and related information with Congress and the public).

130. 18 U.S.C. §§ 2702–2703.

i. Compelled production

I begin with compelled production because providers' terms of service and privacy policies often commit them to limiting the disclosure of user data to a government requester only in response to valid legal process.[131] Providers may well prefer a "friendly" subpoena even if they are otherwise inclined to cooperate with a request.[132] Proceeding under government compulsion ensures that the provider is not exercising discretion in what to disclose, which may shield the provider from potential liability.[133] As a matter of practice, then, providers tend to shy away from giving data away for free.[134]

The SCA's framework for compelled disclosures offers mechanisms for a "governmental entity" to compel the production of information from providers. Section 2703, entitled "Required disclosure of customer communications or records," establishes legal processes that a "governmental entity" may use to compel a provider to disclose data.[135] This framework provides for a three-tiered hierarchy. First, a "governmental entity" may compel a provider to disclose basic subscriber information using a grand jury or administrative subpoena,

---

131. *See, e.g.*, *Privacy Policy*, GOOGLE: PRIV. & TERMS (Feb. 4, 2021), https://policies.google.com/privacy?hl=en-US#infosharing [https://perma.cc/RZT5-M99J] ("For legal reasons[,] [w]e will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosure of the information is reasonably necessary to: Meet any applicable law, regulation, legal process, or enforceable governmental request."). Google's privacy policy purports to "[e]xplain[] what information we collect and why, how we use it, and how to review and update it," whereas its terms of service "describe[s] the rules you agree to when using our services." *Overview*, GOOGLE: PRIV. & TERMS, https://policies.google.com/?hl=en-US [https://perma.cc/9FMV-MVNX].

132. *See, e.g.*, *How Google Handles Government Requests for User Information*, GOOGLE: PRIV. & TERMS, *https://policies.google.com/terms/information-requests* [https://perma.cc/ZK2M-9AQ3] (noting that prior to disclosing user information, Google makes sure a request to disclose satisfies applicable laws; tries to narrow a request if it asks for too much information; and in some cases, objects to producing any information at all).

133. The SCA codifies this concept. *See, e.g.*, 18 U.S.C. § 2707(a), (e).

134. *See supra* note 131 and accompanying text.

135. 18 U.S.C. § 2703. In each scenario, the SCA works in a similar fashion: the governmental entity obtains and serves the legal process on the provider, and in response, the provider searches the records in its possession for responsive information, which it then produces back to the government. Kerr, *User's Guide*, *supra* note 93, at 1219. Even for a warrant, the SCA contemplates a hybrid procedure where the government does not enter the premises to perform a search, but instead functions effectively as a probable-cause subpoena. *See id.* (noting that a § 2703(d) order is a "mix between a subpoena and a search warrant").

which requires a fairly low level of suspicion.[136] Second, it may compel a provider to produce other non-content records pertaining to a customer or subscriber using a court order predicated on reasonable grounds to believe that the information is "relevant and material to an ongoing criminal investigation," a medium level of suspicion.[137] And third, it may compel the production of the contents of a communication or stored file only with a warrant based on probable cause, the highest level of suspicion.[138]

It would be natural to assume that the phrase "governmental entity" covers Congress—after all, it is a branch of the government. There are also some arguable indicia that Congress may have intended § 2703 to be the exclusive method of compelling providers to disclose data, thereby limiting congressional subpoenas.[139]

But in fact, the SCA carves out Congress from the term "governmental entity" altogether, defining "governmental entity" as "a department or agency of the United States or any State or political subdivision thereof."[140] Congress has also codified a default presumption that it is neither a department nor an agency of the United States.[141] Specifically, the statute defines "department" as "one of the executive departments . . . *unless the context shows that such term was intended to describe the executive, legislative, or judicial branches of the government.*"[142] Meanwhile, the statute defines "agency" as "any department, independent establishment, commission, administration, authority, board or bureau of the United States or any corporation in which the United States has a proprietary interest, *unless the context*

136. 18 U.S.C. § 2703(a)–(b).

137. *Id.* § 2703(c)(1)(B), (d).

138. *Id.* § 2703(c)(2).

139. For instance, the title of § 2703 uses the phrase "[r]equired disclosure," perhaps suggesting it is the only mechanism for compelled productions. 18 U.S.C. § 2703. It is also listed as an exception to the prohibitions established in § 2702, perhaps implying that other forms of compulsory process are not exempt. *See infra* Section II.A.2.b (discussing the procedures for compelling production in the law enforcement context).

140. 18 U.S.C. § 2711(4). Congress left the phrase undefined until 2006, when it incorporated the current definition for "governmental entity" in connection with reauthorization of the USA PATRIOT Act. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 107(b)(2)(C), 120 Stat. 192, 202–03 (2006) (defining "governmental entity" as "a department or agency of the United States or any State or political subdivision thereof").

141. 18 U.S.C. § 6.

142. *Id.* (emphasis added).

shows that such term was intended to be used in a more limited sense."[143] In this way, Congress has actually codified congressional exceptionalism in the U.S. Code.

Clearly, Congress would not qualify as an "agency" under this definition, nor as a "department," although the latter is somewhat more nuanced. In particular, the Court has evolved over time in its interpretation of what the showing of "context" requires.[144] That evolution is illustrated in the Court's treatment of 18 U.S.C. § 1001, which prohibits false statements "in any matter within the jurisdiction [of any department or agency] of the Government of the United States."[145]

In its 1955 *United States v. Bramblett*[146] decision, the Court held that 18 U.S.C. § 1001 criminalized making false statements to the Disbursing Office of the House of Representatives, and, by extension, that the term "department" as used in § 1001, "was meant to describe the executive, legislative and judicial branches of the Government."[147] Forty years later, the Court revisited this reasoning in *Hubbard v. United States*,[148] which involved an appeal from a § 1001 conviction for making false statements in papers filed with a court during a bankruptcy proceeding.[149] Calling *Bramblett* a "seriously flawed decision," the Court held that the plain language of § 1001 did not apply to either the legislative or judicial branches.[150] The Court explained that "'[s]hows' is a strong word," and requires "fairly powerful" context to overcome the presumptive definitions of section 6.[151]

The *Bramblett* and *Hubbard* evolution is helpful to interpret the SCA.[152] For one thing, unlike § 1001, the SCA had no statutory

143. *Id.* (emphasis added).

144. *Compare* United States v. Bramblett, 348 U.S. 503, 509 (1955) (concluding the term "department" described the executive, legislative, and judicial branches of the government), *with* Hubbard v. United States, 514 U.S. 695, 702, 715 (1995) (concluding the term "department" did not apply to either the legislative or judicial branches).

145. 18 U.S.C. § 1001 (1948) (amended 1996).

146. 348 U.S. 503 (1955), *overruled by* Hubbard v. United States, 514 U.S. 695 (1995).

147. *Id.* at 509.

148. 514 U.S. 695 (1995).

149. *Id.* at 697.

150. *Id.* at 702, 715, 717.

151. *Id.* at 700.

152. Following *Hubbard*, Congress enacted a criminal prohibition against false statements during a congressional proceeding. *See* False Statements Accountability Act of 1996, Pub. L. No. 104-292, 110 Stat. 3459 (1996).

predecessor; therefore, there is no competing interpretation to the section 6 definition. Further, much like § 1001 and the RFPA, the text of § 2703 bears no affirmative indication that its reach should apply to Congress.[153] There is no express or implied reference to congressional subpoenas, or to Congress itself.[154] Further, the statements of purpose accompanying the House and Senate reports for ECPA contemplate law enforcement, not congressional authorities.[155] For example, the House report states that the purpose of the law was to provide procedures for access to digital evidence by "federal law enforcement officers."[156] In addition, both the House and Senate reports describe ECPA as "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[157] Neither gives any consideration to curtailing congressional subpoenas.

The result seems straightforward, but you do not even need to conclude that the SCA expressly *exempts* Congress to agree that Congress is, in fact, exempted. Rather, you need only observe that § 2703 lacks the necessary language to expressly *include* Congress, or, in other words, that it leaves ambiguity. If that is the case, then the question should simply be whether the SCA should read as impliedly repealing Congress's compulsory authority. For the reasons discussed above, it should not.

ii. Voluntary disclosures

Of course, § 2703 is not the only relevant part of the SCA. Section 2702 of the SCA creates a bar on voluntary disclosures that courts have read in tandem with § 2703.[158] The SCA divides these disclosures into two categories: content information,[159] like emails and messaging, and non-content information, like to and from address information,

153. 18 U.S.C. § 1001; *supra* note 109–18 and accompanying text.

154. *See* 18 U.S.C. § 2703 (referring to a governmental entity, rather than to Congress).

155. *See* S. REP. NO. 99-541, at 3 (1986) (noting the privacy threat posed by "overzealous law enforcement agencies, industrial spies and private parties"); H.R. REP. NO. 99-647, at 16 (1986) (emphasizing that its purpose was to provide procedures for access to and interception of communications by "federal law enforcement officers").

156. H.R. REP. NO. 99-647, at 19 (1986).

157. S. REP. NO. 99-541, at 5 (1986).

158. 18 U.S.C. § 2703.

159. The SCA borrows the definition of "contents" set forth in the Wiretap Act. *See* 18 U.S.C. § 2711(1) (referencing 18 U.S.C. § 2510(8), which defines contents as including "any information concerning the substance, purport, or meaning of that communication").

location data, session logs, subscriber data, and the like. These statutory limitations vary with the perceived privacy interest of the data, namely whether the information falls into a content or non-content category.[160] As to content information, the SCA prohibits disclosure to "*any person or entity*,"[161] and as to non-content information,[162] the SCA only prohibits disclosure to "*any governmental entity*,"[163] which as discussed, is limited to executive branch departments and agencies. In the interest of redundancy, the SCA expressly permits voluntary disclosure of non-content data "to any person other than a governmental entity."[164] No such language exists for content data.

Section 2702's distinction between voluntary disclosures of content and non-content data has implications for compelled disclosures as well. For example, courts have concluded that a civil litigant—because it is not a "governmental entity"—is not barred from using a civil subpoena to gather information from a provider, to the extent that information is non-content data.[165] The SCA permits a foreign government—also not a "governmental entity" under the statute—to use foreign legal process to seek the production of non-content information.[166] But, the SCA prohibits compelled disclosures of *content* information to these same entities based on the restrictions of § 2702.[167]

---

160. *See* U.S.C. § 2702(a) (delineating the protections afforded to the contents of a communication and those afforded to records or other information).

161. 18 U.S.C. § 2702(a)(1)–(2) (emphasis added). The SCA distinguishes between its treatment of content held by an ECS and an RCS in ways that are not relevant here.

162. The statutory language describes this category of information as "a record or other information pertaining to a subscriber to or customer of such service []not including the contents of communications." 18 U.S.C. § 2702(a)(3).

163. 18 U.S.C. § 2702(a)(3) (emphasis added).

164. *Id.* § 2702(b)(6).

165. *See, e.g.*, Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264–65 (S.D.N.Y. 2008) ("But the ECPA does not bar disclosure of non-content data about the private videos (*e.g.*, the number of times each video has been viewed on YouTube.com or made accessible on a third-party website through an 'embedded' link to the video).").

166. *See, e.g.*, Greg Nojeim, *MLAT Reform Proposal: Protecting Metadata*, LAWFARE (Dec. 10, 2015, 2:43 PM), https://www.lawfareblog.com/mlat-reform-proposal-protecting-metadata [https://perma.cc/8XDG-QPQV] (discussing how foreign law enforcement demands for metadata are treated differently under the SCA).

167. *See, e.g.*, Jennifer Daskal & Andrew K. Woods, *A New US-UK Data Sharing Treaty?*, JUST SEC. (June 23, 2015), https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty [https://perma.cc/2J4R-9XAM] (discussing the SCA's application to foreign governments); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 609–11 (E.D. Va. 2008) (addressing the SCA's application to civil litigants).

Under this logic, the SCA would permit a congressional subpoena for non-content information because Congress falls outside the definition of "governmental entity"; however, it would preclude congressional subpoenas for content information. To be clear, even permitting access to non-content information based on a subpoena is already a significant departure from how the SCA treats executive branch requests, which must satisfy a heightened standard for anything beyond basic subscriber information.[168] But, in addition, there is some ambiguity as to whether the content prohibition in fact covers Congress.

By its terms, the content prohibition applies to "any person or entity," which is unquestionably broader than "any governmental entity."[169] "Person" is defined (under the Wiretap Act) as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[170] In the original 1968 enactment of the wiretap prohibition, Congress made clear that while the definition of person "explicitly includes any officer or employee of the United States or any State or political subdivision of a State," it excluded "the governmental units themselves."[171]

Congress made this initial drafting decision against the backdrop of § 1983 civil rights litigation, in which courts had repeatedly held that "person" does not include state or local governments or the United States.[172] Remedying this gap was the stated reason in an otherwise

---

168. *See* 18 U.S.C. § 2703(c)(1) (setting forth requirements a government entity must satisfy, such as obtaining a warrant or court order, before receiving access to non-content information).

169. 18 U.S.C. § 2702(a); *see also* 1 U.S.C. § 1 (defining "person" to include "corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals"). The complete phrase "person or entity" is defined elsewhere, such as in the Lobbying Disclosures Act, as "any individual, corporation, company, foundation, association, labor organization, firm, partnership, society, joint stock company, group of organizations, or State or local government," a definition which excludes Congress and its members. 2 U.S.C. § 1602(14).

170. 18 U.S.C. § 2510(6).

171. S. REP. NO. 90-1097, at 90–91 (1968) ("The definition explicitly includes any officer or employee of the United States or any State or political subdivision of a State. Only the governmental units themselves are excluded. Otherwise, the definition is intended to be comprehensive." (internal citations omitted)).

172. *See* Spock v. United States, 464 F. Supp. 510, 514 n.4 (S.D.N.Y. 1978) (citing Hallinan v. Mitchell, 418 F. Supp. 1056 (N.D. Cal. 1976) (holding that 18 U.S.C. §§ 2510(6) and 2520 did not waive sovereign immunity)) (holding that the United States did not fall within the definition of "person" under the Wiretap Act).

sparse legislative record for adding the term "entity" to the statute in 1986 as part of ECPA, thereby ensuring a statutory right to "recover from any person or entity—including governmental entities—who knowingly or intentionally violated this chapter."[173] From that perspective, Congress did not intend to cover itself at all by the use of the term "entity" in ECPA. Rather, Congress likely intended to make "governmental entities" in the U.S. executive branch, along with state and local governments, amenable to suit.[174]

My point here is not that Congress's ability to obtain content information is clear; rather, my point is that the prohibition *against* the use of congressional process is ambiguous. Textual uncertainty exists because Congress treats itself differently than other government entities, often imposing limits on others' investigative activities that it does not apply to itself, arguably including the prohibitions in § 2702.

This argument is bound to raise some eyebrows, so keep in mind that even if you read the SCA differently in its current form, that language is likely to change. Congress will almost certainly seek to exempt itself explicitly from the SCA if (and when) it decides to amend the statute. For example, the Email Privacy Act,[175] which passed the House *unanimously* and has the support of service providers and privacy advocates, would establish the following "Rule of Construction Related to Congressional Subpoenas":

> Nothing in this section [2703] or in section 2702 shall limit the power of inquiry vested in the Congress by article I of the Constitution of the United States, including the authority to compel the production of a wire or electronic communication (including the contents of a wire or electronic communication) that is stored, held, or maintained by a person or entity that provides remote computing service or electronic communication service.[176]

---

173. S. REP. NO. 99-541, at 43 (1986). At least one federal district court has found that this language did not waive sovereign immunity. *See* Asmar v. IRS, 680 F. Supp. 248, 250–51 (E.D. Mich. 1987) (interpreting similar language as "run[ning] counter to the Supreme Court's tendency to require a specific statutory waiver of sovereign immunity before holding that the United States has consented to suit").

174. There is no question that ECPA created liability for the United States as it was originally enacted. Congress removed "United States" from the scope of liability in 2001 under the USA PATRIOT Act. *See* Seitz v. City of Elgin, 719 F.3d 654, 656 (7th Cir. 2013) (discussing the legislative history of the Wiretap Act's civil cause of action with respect to lawsuits against the "United States").

175. H.R. 387, 115th Cong. (2017).

176. *Id.* § 3(j).

This rule of construction would, in effect, make explicit Congress's authority to obtain the contents of a communication using only a congressional subpoena.

To take a step back from these technical statutory issues, the practical implications are critical. The ability to compel the production of content data is significant because, other than for law enforcement, that authority does not exist.[177] Additionally, it would make this information available to Congress through a subpoena, whereas the executive branch must first satisfy the probable cause standard.

Even the most conservative reading of the SCA, as it now stands, permits Congress to obtain all forms of non-content data through its subpoena power.[178] This information includes the "to" and "from" addressing information in emails, text messages, and chat applications; session logs and IP addresses; subscriber information; and even location data—information that has the potential to reveal the details of an individual's private life and may itself be subject to Fourth Amendment protections.[179] Again, Congress may obtain this information with a subpoena, without following the requirements of § 2703.[180] In sum, the SCA offers a clear signal that the traditional surveillance limits may not apply to congressional surveillance in the way they do to other forms of government surveillance.

2. Fourth Amendment privacy

Theories of the Fourth Amendment in the digital space are rich in their application to law enforcement and national security. One of the most pressing questions has been whether, and why, the Fourth Amendment's warrant requirement applies to the government's constructive searches of digital information. That issue was seemingly resolved in *Carpenter v. United States*,[181] in which the Supreme Court held that a warrant was required for historical cell-site location information,[182] and *Warshak v. United States*[183] before that, in which the

177. *See* 18 U.S.C. § 2703.

178. 18 U.S.C. § 2702(a)(3), (c)(6).

179. *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (holding that Cell Site Location Information (CSLI) is subject to Fourth Amendment protections because it divulges an "all-encompassing record of the holder's whereabouts").

180. *See supra* Section II.A.1.b.i.

181. 138 S. Ct. 2206 (2018).

182. *Id.* at 2220–21.

183. 490 F.3d 455 (6th Cir. 2007).

Sixth Circuit held similarly as to emails.[184] The Fourth Amendment's treatment of congressional searches is largely overlooked, and even more so how it might govern Congress's compelled production of communications data. Yet, the Court's Fourth Amendment decisions treat Congress in a unique way, applying a deferential reasonableness standard that is inconsistent with *Carpenter* and *Warshak*'s categorical warrant requirement.

a. Fourth Amendment exceptionalism

The Bill of Rights, at a very general level, applies to Congress as a state actor, just as it does to the executive.[185] There is a well-established track record for civil liberties challenges to congressional investigations. Recipients of congressional subpoenas have raised First Amendment[186] and Fifth Amendment[187] challenges, and both have resonated in the courts.[188]

Courts have also entertained a handful of Fourth Amendment challenges to congressional subpoenas. However, these Fourth Amendment decisions have approached the subpoena as a "constructive" search, scrutinizing the subpoena's breadth under a reasonableness regime in lieu of imposing (or even contemplating) a strict warrant requirement. For example, in *Oklahoma Press Publishing Co. v. Walling*,[189] the Court explained the Fourth Amendment's treatment of a constructive search effected by a congressional subpoena:

---

184. *Id.* at 475.

185. Watkins v. United States, 354 U.S. 178, 187–88 (1957) ("The Bill of Rights is applicable . . . to all forms of governmental action.").

186. Barenblatt v. United States, 360 U.S. 109, 126 (1959) (holding that when a First Amendment principle is implicated by witness testimony, courts will balance "competing private and public interests at stake"); *see also* Branzburg v. Hayes, 408 U.S. 665, 699–700 (1972) (raising First Amendment challenges to a congressional subpoena); Gibson v. Florida Legis. Investigation Comm., 372 U.S. 539, 546 (1963) (analyzing competing claims of government and individual First Amendment interests); United States v. Rumely, 345 U.S. 41, 42–43 (1953) (examining Congress's investigative power to compel witnesses to testify).

187. The Court has acknowledged that the Fifth Amendment's Due Process Clause plays a role in protecting the rights of witnesses called before Congress. *Watkins*, 354 U.S. at 195–96, 208. Witnesses may also invoke their Fifth Amendment privilege against self-incrimination as a defense to testifying.

188. *See, e.g.*, *id.* at 197–99 ("We cannot simply assume, however, that every congressional investigation is justified by a public need that overbalances any private rights affected.").

189. 327 U.S. 186 (1946).

> The requirement of 'probable cause, supported by oath or affirmation,' literally applicable in the case of a warrant, is satisfied in that of an order for production by the court's determination that the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry. Beyond this the requirement of reasonableness, including particularity in 'describing the place to be searched, and the persons or things to be seized,' also literally applicable to warrants, comes down to specification of the documents to be produced adequate, but not excessive, for the purposes of the relevant inquiry.[190]

Oklahoma Press therefore established that, in lieu of a warrant, the Fourth Amendment requires of Congress only a subpoena relevant to an authorized investigation.[191] As to reasonableness and particularity, the subpoena must adequately specify the materials to be produced. But the decision is equally important for what it does *not* require. Under *Oklahoma Press*, there is no formal "warrant" requirement for Congress, no application or affidavit to submit to a neutral and detached magistrate, and none of the other bells and whistles that normally accompany such a process.[192]

In subsequent decisions, the Court has reiterated that the Fourth Amendment "is not confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process."[193] Yet, the Court has had limited occasion to apply this standard to congressional demands, and when it has, its rulings have suggested a relatively lenient standard. In one such case, *McPhaul v. United States*,[194] the Court considered a conviction for contempt of Congress based on subpoena non-compliance.[195] The defendant argued that the subpoena was "so broad as to constitute an unreasonable search and seizure in violation of the Fourth

---

190. *Id.* at 209 (citing Hale v. Henkel, 201 U.S. 43 (1906); Wilson v. United States, 221 U.S. 361 (1911); Smith v. Interstate Com. Comm'n, 245 U.S. 33 (1917); Balt. & Ohio R.R. Co. v. Interstate Com. Comm'n, 221 U.S. 612 (1911); Interstate Com. Comm'n v. Goodrich Transit Co., 224 U.S. 194 (1912); Harriman v. Interstate Com. Comm'n, 211 U.S. 407 (1908)) (holding that Fourth Amendment applied to administrative subpoenas duces tecum issued in an administrative investigation into violations of the Fair Labor Standards and upholding subpoenas as "reasonable" and not overbroad).

191. *Id.* at 214.

192. *Id.* at 208–09.

193. United States v. Morton Salt Co., 338 U.S. 632, 651–52 (1950).

194. 364 U.S. 372 (1960).

195. *Id.* at 373.

Amendment of the Constitution."[196] The Court dismissed the challenge because the defendant had not informed the committee of his objection, but it also concluded that the congressional inquiry itself was so broad that "the permissible scope of materials that could reasonably be sought was necessarily equally broad."[197]

The effect of *Oklahoma Press* and *McPhaul* is two-fold. First, it ties Fourth Amendment "reasonableness" to the investigation Congress has identified—an investigation that, as described in Part I, a court cannot second-guess if the investigation serves a valid Article I purpose and that may be as broad as Congress's interest in legislation or oversight.[198] Second, it applies a traditional subpoena standard of overbreadth—a standard that, as Christopher Slobogin has aptly characterized, makes subpoenas "extremely easy to enforce."[199] In many ways, then, the Fourth Amendment treatment of congressional subpoenas still resides in the pre-*Warshak*, pre-*Carpenter* era. This begs the question of whether those cases alter the calculus of a congressional demand for user data that implicates the Fourth Amendment, which I turn to next.

b. Congress's digital searches

Recent court decisions firmly establish that the Fourth Amendment applies to constructive searches in the digital space; however, they do not specifically address congressional subpoenas. This Section considers the recent decision in *Carpenter*, in which the Court resolved two issues: first, as to the scope of the Fourth Amendment, whether the compelled production of location information may constitute a constructive search in some cases (it may); and second, as to the requirements of the Fourth Amendment, whether law enforcement officers must obtain a warrant (they must).[200] While *Carpenter* addressed the compelled production of detailed location information

196. *Id.* at 382.

197. *Id.* at 382–83. There are nevertheless limits, and "blanket" subpoenas cross them. *See, e.g.*, Hearst v. Black, 87 F.2d 68, 71 (D.C. Cir. 1936) (holding that a subpoena for all telegraph messages transmitted over a seven-month period through D.C.-area telegraph companies violated the Fourth Amendment).

198. *See supra* Part I.

199. Slobogin, *supra* note 48, at 806.

200. Carpenter v. United States, 138 S. Ct. 2206, 2216, 2221 (2018).

by law enforcement, the implications for congressional subpoenas are less clear but equally important.[201]

As to the first issue—the scope of the Fourth Amendment—*Carpenter*'s holding indicates that a congressional subpoena for location information should be assessed as a constructive search.[202] Post-*Carpenter*, such an application of the Fourth Amendment seems uncontroversial. After all, the process used in each scenario is functionally indistinguishable: like the court order in *Carpenter*, a congressional subpoena compels the provider to collect and produce information, although it does not entail a physical search or seizure.[203] In other words, the "scope" of the Fourth Amendment is, at least in theory, agnostic as to the purpose of the search and the identity of the searcher.

Extending this part of *Carpenter* to a congressional subpoena presents the second, more challenging issue of what the Fourth Amendment requires. Following *Oklahoma Press*, the Court is yet to impose a categorical warrant requirement on Congress, and there are several arguments not to assume that *Carpenter* has established one here.

First, *Carpenter* dealt with a law enforcement search and not a congressional subpoena—a distinction that the Fourth Amendment case law takes seriously. For instance, the Court has long treated law enforcement searches as categorically different than administrative searches or special needs searches.[204] So, when the Court said that

---

201. This Section does not specifically discuss *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), a Sixth Circuit case commonly cited for the proposition that the contents of provider-stored emails are protected by the Fourth Amendment, because *Carpenter* is inclusive of and more recent than *Warshak* and was decided by the Supreme Court.

202. *Carpenter* did not overrule decisions holding that the compelled production of data exhibiting lesser privacy interests, such as a shorter period of location information or basic subscriber and IP address information. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (holding subscriber information not protected by Fourth Amendment); United States v. Forrester, 512 F.3d 500, 505, 510–11 (9th Cir. 2008) (holding IP address information not protected by Fourth Amendment).

203. There might be some practical questions as to whether the production would, in fact, mirror law enforcement processes. For example, when law enforcement applies for a warrant for email, the provider produces the account information, which law enforcement then examines to cull out responsive information. This removes the provider from the position of determining which documents are specifically responsive to the demand.

204. *Compare* New York v. Burger, 482 U.S. 691, 702 (1987) (holding administrative searches can be conducted without a warrant where there is a substantial governmental

"warrantless searches are typically unreasonable where 'a search is undertaken by *law enforcement officials* to discover evidence of *criminal wrongdoing*,'"[205] it was specifically invoking the Fourth Amendment's categorical treatment of a law enforcement search.[206] It was not, however, commenting on other invasions of privacy that serve markedly different governmental interests, particularly legislative, oversight fact-finding, or even impeachment.[207] Of course, had the Court intended to extend its holding to Congress, it would also have had to address its holding in *Oklahoma Press*, which as of now is undisturbed.

Second, doctrinal points aside, it is challenging to imagine whether *Carpenter* required Congress, as a matter of Fourth Amendment procedure, to apply to an Article III court for permission to issue a subpoena. Such a process would place the judiciary into a pre-enforcement supervisory role over Congress's investigative decisions. That kind of dynamic is difficult to square with the constitutional scheme (it certainly has no precedent), and the Court has suggested it might not even be permitted.[208] But in any event, cases like *Warshak* have acknowledged that the heightened warrant requirement can be "offset" by judicial review prior to the imposition of sanctions for non-compliance,[209] a mechanism that is available to providers that are

---

interest in regulation), *and* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (finding the warrant requirement impracticable where there is a special need beyond the need for law enforcement in a school), *with* Arizona v. Gant, 556 U.S. 332, 351 (2009) (holding law enforcement officers violated the Fourth Amendment when they searched an arrestee's car without a warrant and the search did not fall into an established exception to the warrant requirement).

205. *Carpenter*, 138 S. Ct. at 2221 (emphasis added) (quoting Vernonia Sch. Dist., 515 U.S. at 653).

206. *See, e.g.*, City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000) (holding that a warrantless narcotics checkpoint program violated the Fourth Amendment because its "primary purpose" was "to advance 'the general interest in crime control'" (quoting Delaware v. Prouse, 440 U.S. 648, 659, n.18 (1979))).

207. *Id.* at 47–48 (emphasizing that this decision is only aimed at the general interest of crime control).

208. *See, e.g.*, Eastland v. U.S. Servicemen's Fund, 421 U.S. 491, 509 (1975) (holding that Speech or Debate Clause precluded a federal court from pre-enforcement injunction of a congressional subpoena); *The Supreme Court, 1974 Term*, 89 HARV. L. REV. 132, 136–38 (1975) (discussing implications of *Eastland*'s holding for pre-enforcement litigation, in contrast to litigation for contempt).

209. Warshak v. United States, 490 F.3d 455, 475 (6th Cir. 2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008); *accord* City of Los Angeles v. Patel, 576 U.S. 409, 421–22 (2015); See v. City of Seattle, 387 U.S. 541, 545 (1967) ("[T]he subpoenaed party may

served a congressional subpoena.[210] Furthermore, in the absence of a gag order, a provider can choose to notify the user of a subpoena, which opens the door for the user to bring a Fourth Amendment challenge.[211]

Admittedly, the notion that the Fourth Amendment requires a heightened form of process for law enforcement access to communications data but not for Congress would seem contrary to current trends. The Court held in a trio of recent opinions that law enforcement must obtain a warrant for slap-on GPS trackers,[212] searches of cell phones incident to arrest,[213] and compelled production of cell site location information.[214] Privacy advocates have promoted a "warrant-for-content" rule for law enforcement access to stored communications.[215] Additionally, courts around the country have presumed that the Fourth Amendment requires a government actor to

---

obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply.").

210. This opportunity would be available as part of a defense to a civil enforcement or contempt proceeding.

211. Under the SCA, investigators may obtain a non-disclosure order from the court that directs a provider not to inform the user of a search warrant or other legal process. The result creates a Fourth Amendment conundrum, because the provider lacks "standing" to challenge the legal process, whereas the user has standing but lacks notice. *See* Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 26 WM. & MARY BILL RTS. J. 437, 439–41 (2017). When Congress operates outside of the SCA's framework, *see supra* Section II.A.1, it may not avail itself of such non-disclosure orders and the "conundrum" is avoided.

212. United States v. Jones, 565 U.S. 400, 404 (2012) (finding a search under the Fourth Amendment where law enforcement installed a GPS device on a vehicle to monitor movements).

213. Riley v. California, 573 U.S. 373, 398, 403 (2014) (acknowledging the privacy interest in cell phones is greater than other items because of the storage capacity and the distinct types of information included).

214. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (emphasizing the "deeply revealing nature of CSLI").

215. *See, e.g.*, *Coalition Letter in Support of Email Privacy Act*, CTR. FOR DEMOCRACY AND TECH. (Apr. 25, 2016), https://cdt.org/insights/coalition-letter-in-support-of-email-privacy-act-april-26 [https://perma.cc/FH9M-EHDB] (advocating for passage of the Email Privacy Act). However, as noted *supra* Section II.B.1, while the Email Privacy Act itself sought to enact a "warrant for content" rule into law, it did not propose to curtail Congress's authorities. *Id.*

obtain a warrant to compel the production of content information since the Sixth Circuit's *Warshak* decision.[216]

Yet after *Carpenter*, continued application of a reasonableness test to congressional subpoenas would not be unprecedented. In fact, it would echo decisions like *Naperville Smart Meter Awareness v. City of Naperville*,[217] which applied a reasonableness balancing test to a city's collection of smart meter data because it was "not performed as part of a criminal investigation."[218] *Naperville* aptly illustrates that, post-*Carpenter*, the Fourth Amendment treats a search for prosecutorial purposes differently than one for other government interests, and therefore *Carpenter* should not be understood to shift the Fourth Amendment's requirements for Congress.[219]

To some, this result would not be altogether surprising, and it might even be consistent with competing trends in Fourth Amendment jurisprudence—that the Fourth Amendment does not categorically require a warrant based on probable cause.[220] Instead, a search or seizure under the Fourth Amendment need only be reasonable, and, separately, if a warrant is issued, it must satisfy the Fourth Amendment's probable cause and particularity standards.[221] Many of

---

216. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that government investigators must use a warrant to obtain provider-controlled emails, even though the SCA only required a subpoena).

217. 900 F.3d 521 (7th Cir. 2018).

218. *Id.* at 527–28. As the Seventh Circuit observed, "Naperville conducts the search with no prosecutorial intent. Employees of the city's public utility—not law enforcement—collect and review the data." *Id.* at 528. Likewise for Congress. Alan Rozenshtein has offered up *Naperville* to illustrate the viability of a Fourth Amendment reasonableness test for law enforcement activity post-*Carpenter*. Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. (2019).

219. *Naperville*, 900 F.3d at 528 (noting the fact that employees of the city collect the data, not law enforcement, "lessens an individual's privacy interest").

220. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 761 (1994) (arguing that the Fourth Amendment does not require warrants or probable cause at all, just reasonableness); *see also* Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonableness Analysis*, 81 MISS. L.J. 1133, 1138–40 (2012) (describing divergence between "warrant preference view" and "separate clauses view" of the Fourth Amendment). *But see* Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 515 (1995) (detailing the legislative history of the Fourth Amendment and showing that, while it prohibits all unreasonable searches and seizures, its general prohibitions targeted only improper warrants).

221. The Fourth Amendment provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, *and* no [w]arrants shall issue, but upon probable cause,

the Court's opinions have echoed this notion,[222] and as others have acknowledged, the Court's decisions have recently moved closer to this "separate clauses" view, not further away.[223]

To sum up, even after *Carpenter*, the Fourth Amendment's protections for a congressional request remain unchanged. Unlike *Carpenter*'s warrant requirement, the case law on constructive searches imposes only an overbreadth standard on congressional subpoenas. In that analysis, the reasonableness of the subpoena is contingent on the scope of the inquiry—if the investigation is broad, the subpoena can be too. In these scenarios, the Fourth Amendment does not require an application to an unbiased magistrate; is satisfied by relevance in lieu of probable cause; and may offer no suppression remedy either.[224]

There is, to be sure, some uncertainty with so little directly applicable case law. Perhaps a constructive search of digital information would merit heightened judicial scrutiny because of the increased privacy interests, or the parties would negotiate restrictions on, say, segregating non-pertinent information or how long Congress can retain information in its records, as I discuss further in Part III.[225] But all of these adjustments would supplement—not replace—the

---

supported by [o]ath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV (emphasis added). The significance of the word "and" separating the reasonableness and warrants clauses is at the heart of this theory.

222. Florida v. Jimeno, 500 U.S. 248, 250–52 (1991) (finding no violation of the Fourth Amendment where consent could "reasonably be understood" to also apply to a container within a car).

223. *See* Lee, *supra* note 221, at 1139–40, 1143 (arguing that the warrant preference view is likely to fade away more since Justice Stevens left the bench).

224. There is no precedent for application of the exclusionary rule to a congressional hearing or investigation, as opposed to a related criminal proceeding (such as, for instance, a prosecution for perjury, contempt, or obstruction), and even as to the latter, it has arisen exceedingly rarely. In *United States v. McSurely*, which involved a contempt conviction for subpoena non-compliance, the court held that the exclusionary rule required suppression *of the subpoenas* because they were predicated on evidence seized in violation of the Fourth Amendment. 473 F.2d 1178, 1191–92 (D.C. Cir. 1972). The court reasoned that the taint of the initial police search extended to the congressional subpoenas, and on that basis reversed the conviction. *See id.* But this reasoning seems questionable, especially under the expanding application of the good faith exception. *See id.* at 1199 (Wilkey, J., concurring in part) (doubting "that a remote hypothetical effect on derivative Congressional use of discovered information could possibly figure significantly in these officials' motivations").

225. *See infra* Part III.

current regime, which is a permissive and highly context-dependent inquiry, and not an area of hard and fast rules.

B. Internal Surveillance Limits

In the absence of external limits, Congress is free to exercise its surveillance authority as far as its "internal limits" permit. *Internal limits* "are the boundaries of Congress's powers taken on their own terms."[226] There are few internal limits on executive branch surveillance,[227] and the same is true of Congress. Based on *McGrain*'s rule that Congress's investigative authority is co-extensive with its expressed Article I powers, then Congress's surveillance capacity extends as far as its authority to legislate, conduct oversight, appropriate, or impeach.[228] In this Section, I describe the surveillance implications of these limits as applied to access to digital information, public disclosures, and the special case of presidential information.

1. Access limits and Mazars

If Congress may exercise its subpoena authority in furtherance of its Article I powers, such as legislation, oversight, and impeachment, what are the limiting principles? As several examples help illustrate, these internal limits tend to reflect separation of powers considerations, not privacy considerations, and courts enforce these limits under highly deferential standards.

---

226. Primus, *supra* note 28, at 578.

227. If we accept that federal law enforcement is endowed with the authority to enforce criminal law, then the "internal" limit on that authority is the scope of criminal law. Because of the expansive scope of the U.S. criminal code, this limitation has been eroded. *See, e.g.*, Julie R. O'Sullivan, *The Federal Criminal "Code" Is A Disgrace: Obstruction Statutes As Case Study*, 96 J. CRIM. L. & CRIMINOLOGY 643, 651–52 (2006) (observing that while "the Constitution contemplates a limited role for federal criminal law," overcriminalization and the "federalization" of criminal law have expanded its presence); John C. Jeffries, Jr. & Hon. John Gleeson, *The Federalization of Organized Crime: Advantages of Federal Prosecution*, 46 HASTINGS L.J. 1095, 1125 (1995) ("With legislation covering virtually any crime they might plausibly wish to prosecute, federal prosecutors pick their targets and marshal their resources, not in response to the limitations of the substantive law but according to their own priorities and agendas.").

228. *See* McGrain v. Daugherty, 273 U.S. 135, 178–79 (1927) (noting Congress has authority to select the means and methods of carrying into effect constitutional powers; *see also, e.g.*, ALISSA M. DOLAN ET AL., CONG. RSCH. SERV., IF10015, CONGRESSIONAL OVERSIGHT AND INVESTIGATIONS (2014) (stating that congressional power over oversight and investigations are "so essential to the legislative function as to be implied" by Article I).

One common refrain, as the Court has put it, is that Congress's power does not extend to a "law enforcement" function"—a power constitutionally reserved "to the Executive and the Judiciary."[229] That is, "Congress may not use subpoenas to 'try' someone 'before [a] committee for any crime or wrongdoing.'"[230] But it is not difficult to reframe a law enforcement inquiry as a legislative one. For example, the FBI might investigate whether a presidential campaign conspired with agents of a foreign government to interfere in the election. Congress might investigate those same events, either to determine whether current law was sufficient to capture or deter the bad behavior or instead to assess whether new laws are needed to address it. Indeed, it is not uncommon to see parallel (and, on occasion, effectively identical) law enforcement and congressional investigations.[231]

Another commonly evoked principle is that Congress does not have a "'general' power to inquire into private affairs and compel disclosures."[232] But, in practice, legislators must understand the specific facts on the ground before crafting new laws, assessing current law, or conducting effective oversight of a particular event. They also must decide whether legislation is necessary or appropriate in the first place, meaning that Congress can investigate even if it never enacts legislation; so too with impeachment.[233] The areas in which Congress

---

229. Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2024 (2020) (quoting and referencing Quinn v. United States, 349 U.S. 155, 161 (1955)). As announced by the Court in *Kilbourn v. Thompson*, Congress may not undertake a "fruitless investigation into the personal affairs of individuals." 103 U.S. 168, 195 (1880).

230. *Mazars*, 140 S. Ct. at 2032 (quoting *McGrain*, 273 U.S. at 179).

231. Watergate and the SSCI investigation into Russian election interference provide two examples. *See, e.g.*, 119 CONG. REC. 3831 (daily ed. Feb. 7, 1973) (noting the establishment of a select committee charged with investigating "the extent, if any, to which illegal, improper, or unethical activities were engaged in by any persons, acting individually or in combination with others, in the presidential election of 1972"); Scott Detrow, *There Are Many Russia Investigations. What Are They All Doing?*, NPR (June 8, 2017, 4:00 AM), https://www.npr.org/2017/06/08/531940912/there-are-many-russia-investigations-what-are-they-all-doing [https://perma.cc/YJ3A-ZTJK]; *see also, e.g.*, Hutcheson v. United States, 369 U.S. 599, 616 (1962) ("Deciding whether acts that are made criminal by state law ought also to be brought within a federal prohibition, if, as here, the subject is a permissible one for federal regulation, turns entirely on legislative inquiry.").

232. *Mazars* 140 S. Ct. at 2032 (emphasis added) (quoting *McGrain*, 273 U.S. at 173–74); *see also* Kilbourn v. Thompson, 103 U.S. 168, 195 (1880) (noting Congress's need to understand what it is investigating).

233. *See* Barenblatt v. United States, 360 U.S. 109, 111 (1959) ("The power of inquiry has been employed by Congress throughout our history, over the whole range

can conceivably act, whether through legislation, oversight, or some other power, are also necessarily broad, both as a function of modern life and the increasing powers and responsibilities of the federal government.[234] As a result, Congress has the corresponding ability to direct its investigative authority almost anywhere, reflecting the "operative reality that the powers of Congress face virtually no internal limits."[235]

Indeed, on the few occasions where the Court has considered the privacy implications of a congressional subpoena and imposed a First Amendment balancing test to weigh such concerns, it has routinely upheld Congress's broad authority to investigate.[236] To the extent it has limited Congress's authority, those decisions have relied instead on *external* limits imposed by Fifth Amendment considerations.[237] Over

---

of the national interests concerning which Congress might legislate or decide upon due investigation not to legislate . . . ."); Eastland v. U. S. Servicemen's Fund, 421 U.S. 491, 509 (1975) ("The very nature of the investigative function—like any research—is that it takes the searchers up some 'blind alleys' and into nonproductive enterprises. To be a valid legislative inquiry there need be no predictable end result.").

234. As the Court put it in *Watkins v. United States*, this includes "surveys of defects in our social, economic or political system for the purpose of enabling the Congress to remedy them." 354 U.S. 178, 187 (1957); *see, e.g.*, U.S. CONST., art. I, § 8, cl. 18 ("The Congress shall have Power . . . To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.").

235. Richard Primus, *Why Enumeration Matters*, 115 MICH. L. REV. 1, 3–5 (2016) (arguing that the enumeration principle, even if not an accurate depiction of "present constitutional reality," reflects an assertion "that the basic structure of American government remains continuous with what was at the beginning").

236. For example, *Watkins* involved a contempt conviction for a witness's refusal to testify about his associates and their political affiliations during the McCarthy era. Consistent with its First Amendment jurisprudence, the Court's balancing test weighed the harm to individual privacy against the government's interest, holding that the conviction would be invalid if the "predominant result" of the inquiry could "only be an invasion of . . . private rights." 354 U.S. at 200. Rather than applying this test, however, the Court overturned the conviction on due process grounds. *Id.* at 209; *see also Barenblatt*, 360 U.S. at 122–23 (declining to apply the *Watkins* balancing test and concluding that the committee's investigative interest outweighed the threat presented by the questioning).

237. Some of these decisions rest on the notion that Congress has provided insufficient notice of the "question under inquiry." *Watkins*, 354 U.S. at 213; *see also* Flaxer v. United States, 358 U.S. 147, 151 (1958) (noting a witness must have reasonable notice to supply a congressional committee with requested information). Others rest on the right against self-incrimination. *See, e.g.*, Quinn v. United States, 349

time, the Court has sidelined the notion that some "private affairs" existed beyond Congress's inquisitive eye.[238] As Saikrishna Bangalore puts it, "[t]he prototypical exercise of 'legislative power' generates laws regulating private conduct,"[239] which makes investigations of private conduct unavoidable.

One complicating factor is that courts grant significant deference to Congress's legislative and investigative decisions.[240] That is, if Congress has determined that an area may be worth investigating for legislative or oversight purposes, it is not the courts' role to second-guess that decision.[241] As a result, courts have been unwilling, in most cases, to "challenge the wisdom of Congress' [sic] use of its investigative authority."[242] Indeed, the Court has generally avoided a requirement that Congress identify at the outset a legislative topic of interest, or that it even intends to legislate.[243] Instead, the Court has indulged a presumption that Congress's investigative demands are in pursuit of a

---

U.S. 155, 164–65 (1955) (acknowledging a witness' ability to invoke the Fifth Amendment against self-incrimination during a congressional investigation).

238. This can be traced through the Court's treatment of the *Kilbourn* decision. *See* 103 U.S. at 194–96 (finding a subpoena unenforceable because the investigation was "of a judicial nature" concerning "private affairs"); *In re* Chapman, 166 U.S. 661, 668 (1897) (holding that probe of a stockbroker's business was not an unreasonable search into the broker's private affairs); McGrain v. Daugherty, 273 U.S. 135, 173 (1927) (recognizing that "neither house is invested with '*general*' power to inquire into private affairs and compel disclosures" (emphasis added)); Sinclair v. United States, 279 U.S. 263, 294 (1929) (upholding a contempt conviction where the subpoena was not "related *merely* to . . . private or personal affairs" (emphasis added)).

239. Prakash, *supra* note 33, at 809. Richard Primus has similarly observed that Congress can "regulate pretty much anything that a state could regulate." Primus, *supra* note 236, at 2.

240. *See* CHRISTOPHER M. DAVIS ET AL., *supra* note 101, at 34 (noting what constitutes permissive legislative purpose is broad).

241. *See, e.g.*, Hutcheson v. United States, 369 U.S. 599, 622 (1962) (reasoning the Constitution imposes on the judiciary the duty of not lightly interfering with Congress's legitimate exercise of its powers).

242. Eastland v. U.S. Servicemen's Fund, 421 U.S. 491, 511 (1975). The Court warned against judicial second-guessing of this sort, noting that the Speech or Debate Clause "was written to prevent the need to be confronted by such 'questioning.'" *Id.*

243. *See* CONG. RSCH. SERV., *supra* note 101, at 34 (noting the Supreme Court has sometimes presumed that committees act with legislative purpose when investigating government activity).

legitimate purpose.[244] The Speech or Debate Clause[245] acts as a further cloak for Congress's investigative decisions, limiting a court's ability to peek behind the curtain of Congress's stated purpose. As a result, courts may not even examine Congress's underlying motives.[246]

Overall, this leaves significant discretion for Congress in the surveillance space, internal limits notwithstanding. Thus, the Court emphasized in *Barenblatt v. United States*,[247] another decision addressing a McCarthy-era conviction for contempt of Congress, that constraints against the potential abuse of Congress's power ultimately lie in politics, not law: "in the people, upon whom, after all, under our institutions, reliance must be placed for the correction of abuses committed in the exercise of a lawful power."[248] In effect, *Barenblatt* admits that these internal limits are insufficient to protect privacy, but that checking this excess is for the political, not the judicial, system.[249]

All told, these forgiving internal limits give Congress significant leeway to exercise its investigative power to access and disclose user data. That is, with one limited exception: the special case of presidential information addressed in *Trump v. Mazars USA, LLP*.[250]

In *Mazars*, the Court adopted a heightened standard for reviewing the use of Congress's subpoena authority to obtain the President's personal records from a third-party entity.[251] Faced with various subpoenas to financial institutions for President Trump's tax records,

---

244. *See, e.g.*, McGrain v. Daugherty, 273 U.S. 135, 178 (1927) (holding that a direct avowal that Congress's purpose was to aid in legislating is preferred, but "not indispensable"); *In re* Chapman, 166 U.S. 661, 670 (1897) (finding advance notice of Senate intent at the conclusion of the investigation was unnecessary).

245. U.S. CONST. art. I § 6, cl. 1.

246. *See, e.g.*, Barenblatt v. United States, 360 U.S. 109, 132 (1959) (holding that the judiciary lacks authority to intervene based on the motives that spur Congress's constitutional acts in pursuance of its constitutional powers).

247. *Id.*

248. *Id.* at 133 (quoting McCray v. United States, 195 U.S. 27, 55 (1904)).

249. *See id.* at 132–33 (finding that "[t]he remedy" for an improper Congressional inquiry lies "in the people" (quoting McCray v. United States, 195 U.S. 27, 55 (1904)).

250. 140 S. Ct. 2019, 2036 (2020); *see also* CONG. RSCH. SERV., *supra* note 101, at 37 (stating that when investigating the President, judicial deference to legislative purpose gives way to greater scrutiny).

251. *See Mazars*, 140 S. Ct. at 2036 ("[T]o narrow the scope of possible conflict between the branches, courts should insist on a subpoena no broader than reasonably necessary to support Congress's legislative objective. The specificity of the subpoena's request 'serves as an important safeguard against unnecessary intrusion into the operation of the Office of the President.'" (quoting Cheney v. U.S. Dist. Court for the Dist. of Columbia, 542 U.S. 367 (2004))).

the Court declined to defer to Congress's judgment about legislative purpose and need.[252] Instead, under *Mazars*, a court must consider not just the "significant legislative interests of Congress," but also the "unique position" of the President.[253] In doing so, *Mazars* instructs a court to assess (1) "whether the asserted legislative purpose warrants the significant step of involving the President and his papers"; (2) whether the subpoena is "no broader than reasonably necessary to support Congress's legislative objective"; (3) if Congress has offered "detailed and substantial" evidence of its legislative purpose; and (4) whether the "burdens imposed on the President" lead to "institutional advantage."[254]

I discuss *Mazars* and its implications for congressional surveillance in more detail in Part III.[255] It is worth noting here, however, that the Court was motivated in part by the prospect of Congress declaring "open season" on information held by third-party providers.[256] To provide context for its concerns, the Court cited *Carpenter v. United States*, a Fourth Amendment case involving law enforcement access to cell site location information.[257] Given the potentially broad scope of congressional access to third-party data, however, *Mazars* creates only a narrow exception to the deferential treatment described above.[258] For example, it does not address demands for *non-presidential* information (such as other federal officials or private individuals), *metadata* (non-content records about user activity), or *non-legislative* subpoenas (such as subpoenas for oversight and impeachment). As a result, *Mazars* leaves the treatment of congressional surveillance largely unresolved.

2. Disclosure limits

Similarly, there are few limits on Congress's ability to disclose information it obtains through its investigations. For the executive branch, there are a variety of protections against disclosure of private

252. *See id.* at 234 (reasoning that without limits to Congress's subpoena powers, Congress could inflate itself at the expense of the President).

253. *Id.* at 2035.

254. *Id.* at 2035–36.

255. *See infra*, Part III.

256. *Mazars*, 140 S. Ct. at 2035 (referencing "information held by schools, archives, internet service providers, e-mail clients, and financial institutions").

257. *Id.* at 2219–20.

258. *See supra* notes 251–55 and accompanying text.

information, although they can be manipulated.[259] There are, for instance, secrecy rules governing the grand jury,[260] non-disclosure orders that courts can impose,[261] and special obligations with respect to classified information, including the potential for criminal sanctions.[262] But many of these rules are not applicable to Congress, and certain aspects of Congress's work necessitate the freedom to share information with the public.[263] In other words, Congress's Article I responsibilities again establish few internal limits on disclosure, and exposure is often a purpose (if not *the* purpose) of congressional investigations.[264]

There are at least two reasons for this dynamic. First, the "informing function" plays a valuable role in Congress's core legislative and oversight duties, among others.[265] In furtherance of those responsibilities, Congress regularly publishes investigative reports and legislative findings, issues press releases, engages with the media, and members communicate directly with their constituents.[266] Such disclosures provide critical transparency to the public about how the executive branch exercises its authorities, conveys the basis for Congress's legislative and oversight decisions, and apprises voters of how their elected representatives are fulfilling—or not fulfilling—their goals. An informed public is a core component of democracy,[267] and

---

259. For a comprehensive treatment of plants, leaks, and "pleaks" within the executive branch, *see generally* David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 HARV. L. REV. 512 (2013) (reviewing the "leaks" in the regulatory regime leading to disclosure of secret government information).

260. *See* FED. R. CRIM. P. 6(e).

261. 18 U.S.C. § 2705(b).

262. *Id.* § 793.

263. *See* CONG. RSCH. SERV., R41079, CONGRESSIONAL OVERSIGHT: AN OVERVIEW 6 (stating a central function of representative government is for the people to bring realities to the light and demand accountability from those in power).

264. *See, e.g.*, *id.* (noting that informing the public is central to Article I congressional functions).

265. *See* WOODROW WILSON, CONGRESSIONAL GOVERNMENT: A STUDY IN AMERICAN POLITICS 303 (Transaction Publishers 2002) (1900) (stating the duty of a representative body is to diligently examine government affairs and inform on what it finds).

266. *See* Josh Chafetz, *Congressional Overspeech*, 89 FORDHAM L. REV. 529, 556 (arguing that "the communicative use of oversight tools has often served as a significant driving force in American constitutional politics").

267. *See, e.g.*, Doe v. McMillan, 412 U.S. 306, 332 (1973) (Blackmun, J., concurring in part and dissenting in part) (reasoning when Congress publishes a report, its object

as a result, it is difficult to separate Congress's disclosures from a legislative or oversight purpose.

Second, the Speech or Debate Clause provides absolute immunity to members of Congress and their staff for legislative acts.[268] For example, a senator can disclose the alleged identity of a federal whistleblower on the chamber floor and online without any apparent legal repercussions.[269] Further, a court may not block disclosure of information that is part of the legislative process.[270] Courts have also granted Congress a presumption of regularity in handling the information it possesses, meaning interested parties cannot challenge an unlawful disclosure they merely believe *might* occur.[271] For instance, in a challenge to the possible disclosure of trade secrets, the D.C. Circuit held that once the documents were in congressional hands, "courts must presume that the committees of Congress will exercise

---

was not only to advice other members of Congress, but also to advice the public of proposed legislation and problems, and to allow the public to evaluate the performance of their elected representatives). In this spirit, Senator Ervin, who chaired the Senate Select Committee on Presidential Campaign Activities, remarked in the introduction of THE POWER TO PROBE: "[F]ulfilling its responsibility to inform the public about the state of government is one of Congress's most significant functions. It is a crucial responsibility if the people are to participate in the democratic process. The people govern best when fully informed." Sam J. Ervin, Jr., Introduction to JAMES HAMILTON, THE POWER TO PROBE, at xiii (1976).

268. The Speech or Debate Clause provides: "[F]or any Speech or Debate in either House, [Senators and Representatives] shall not be questioned in any other Place." U.S. CONST. Art. 1, § 6, cl. 1. *See* Eastland v. U.S. Servicemen's Fund, 421 U.S. 491, 502–03 (1975) (holding that when legislatures act within the sphere of legitimate legislative activity, their actions are protected from litigation).

269. *See* Bess Levin, *Rand Paul Outs Alleged Whistleblower to Spite John Roberts*, VANITY FAIR: LEVIN REPORT (Jan. 30, 2020), https://www.vanityfair.com/news/2020/01/rand-paul-whistleblower-impeachment [https://perma.cc/2YTR-H55X] (examining Senator Rand Paul's decision to oust the supposed whistleblower who complained against Donald Trump).

270. *See* McMillan, 412 U.S. at 317–18 (discussing the Speech and Debate Clause, including protection for Congressional Committees when they conduct hearings, prepare reports, and publicize reports); Gravel v. United States, 408 U.S. 606, 615 (1972) (finding members of Congress's speech and debate in either house is privileged).

271. *See, e.g.*, CONG. RSCH. SERV., *supra* note 101, at 59 ("The Supreme Court has made clear that the mere fact that the *contents* of a document may be incriminating does not mean that the document itself is protected from disclosure [in the context of a Congressional investigation] under the Fifth Amendment.").

their powers responsibly and with due regard for the rights of affected parties."[272]

C. Procedural Surveillance Limits

As I have explained so far, there are surprisingly weak constraints on Congress's ability to direct its investigative powers toward surveillance. Despite this, Congress has not exercised its surveillance tools until recently, and when it has, Congress has restrained the number and scope of its requests.[273] In some cases, Congress's choice not to use surveillance authorities has played out publicly.[274] Senate Republicans, for example, chose not to pursue a subpoena for Congressman Adam Schiff's and then-candidate Joe Biden's phone records, despite calls by some to do so following the House impeachment report.[275] This self-restraint arises from procedural rules that govern issuance and enforcement of congressional subpoenas and the political checks that can constrain its surveillance authority, or *process limits*.[276]

---

272. Exxon Corp. v. FTC, 589 F.2d 582, 589 (D.C. Cir. 1978) (citing Ashland Oil, Inc. v. FTC, 548 F.2d 977, 979 (D.C. Cir. 1976)).

273. *See, e.g.*, SSCI REPORT, *supra* note 1, at 5 (noting the Senate Intelligence Committee's report on Russian interference in the 2016 election only investigated "the extent of Russian activities," and the response of the U.S. Government).

274. *See, e.g.*, Peter Overby, *Democrats Vow to Rein in Trump Administration If They Win the House*, NPR (Oct. 24, 2018, 5:00 AM), https://www.npr.org/2018/10/24/657477478/democrats-vow-to-rein-in-trump-administration-if-they-win-the-house [https://perma.cc/WX27-NPKL] (claiming new oversight by House Democrats after the 2018 mid-terms would mark an abrupt change for Congress, which while predominantly Republican, resisted investigating alleged wrongdoings by officials and Trump's possible conflicts of interest).

275. *See generally* Olivia Beavers, *GOP Member Urges Graham to Subpoena Schiff, Biden Phone Records*, HILL (Dec. 4, 2019, 3:08 PM), https://thehill.com/homenews/house/473047-gop-member-urges-graham-to-subpoena-schiff-biden-phone-records [https://perma.cc/YGS4-2JGV] (reporting on House Republican pressure on Senator Lindsey Graham to subpoena the call records of top Democrats and a whistleblower lawyer); Cat Zakrzewski, *The Technology 202: Phone Records from AT&T and Verizon Obtained in Impeachment Inquiry Spark Controversy*, WASH. POST (Dec. 6, 2019, 9:14 AM) https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/12/06/the-technology-202-phone-records-from-at-t-and-verizon-obtained-in-impeachment-inquiry-spark-controversy/5de93d5188e0fa652bbbdc1e [https://perma.cc/K2YG-Z3KR] (reporting on phone logs subpoenaed from Verizon and AT&T of Trump's personal attorney, Rudolph W. Giuliani).

276. For a different take on whether process limits constrain Congress from pursuing investigations of the President, *see* Marshall, *supra* note 57, at 803 (arguing that "[p]rocess requirements . . . do not impose a major constraint on Congress's use of its investigative power"). Despite Marshall's position, I argue here that surveillance

Process limits can compensate for weak internal limits and provide an essential supplement to external limits. As Richard Primus puts it: "process limits do not place particular substantive outcomes wholly out of reach. But they raise the cost of federal action, thus diminishing the likelihood that Congress will do any particular thing, especially any particular thing that might arouse substantial opposition."[277] In this Section, I argue that Congress's unique process limits offer meaningful, even if imperfect, constraints on congressional surveillance.

1. Process as a limit

Process limits on surveillance offer several advantages over the substantive limits I have already described. *First*, process applies independent of internal and external constraints. That is, government entities must follow process rules regardless of whether, for instance, the resulting conduct qualifies as a search under the Fourth Amendment or whether it is subject to statutory protections under the SCA.[278] *Second*, process can create transparency and accountability in government decision making. That is, it offers a metric by which to judge a government actor's adherence to an objective, pre-determined path, and it creates opportunities for the public to sway government actors in their choices.[279] *Third*, process creates costs, and government actors must weigh these costs against the benefit they anticipate from conducting surveillance.[280]

Of course, process limits exist in executive surveillance, but they rarely provide transparency. For instance, as Barry Friedman and Maria Ponomarenko observe, processes for *adoption* of surveillance

---

subpoenas are categorically different and that process limits impose greater constraints on them.

277. Primus, *supra* note 28, at 579.

278. *Cf.* Slobogin, *supra* note 19, at 97 ("[T]he hard look standard [of administrative law] applies regardless of whether the government program is designated a Fourth Amendment 'search' or 'seizure.'").

279. Abbe R. Gluck et al., *Unorthodox Lawmaking, Unorthodox Rulemaking*, 115 COLUM. L. REV. 1789, 1839–43 (discussing implications of non-traditional lawmaking for democratic accountability, transparency, and public input).

280. *See* Slobogin, *supra* note 19, at 134 (noting objectives of the Administrative Procedures Act such as "(1) to subject agency actions to public scrutiny; (2) to establish requirements for rulemaking and adjudication; and (3) to provide a method of challenging agency action in court on constitutional or statutory grounds, including claims that the APA itself has been violated"); Rozenshtein, *supra* note 20, at 133–34 (discussing effects of litigation by providers against government demands for data).

authorities by the police are often "divorced from "transparent democratic processes such as legislative authorization and public rulemaking," features that create additional transparency and accountability[281] and, therefore, raise the costs of adopting controversial surveillance practices.[282] As Paul Ohm recognizes, the same is true of internal agency deliberations over the interpretation of surveillance laws.[283]

As to the *use* of surveillance authorities, there is often little public information about basic aspects of what law enforcement does, especially in real time. Applications for warrants or court orders are made *ex parte* and subject to non-disclosure orders, and grand jury secrecy applies to subpoena returns and witness testimony.[284] To a degree, this is a necessary feature of a criminal investigation because exposing too much information about investigative practices simply tells criminals how not to get caught. National security surveillance is shrouded in even more secrecy. But as a consequence, the public has little insight into how the executive branch uses surveillance.[285] For example, information about law enforcement requests to providers often does not come from the government, but rather from the providers themselves.[286] And the details of specific investigative techniques, such as government "hacking," frequently come to light

---

281. Friedman & Ponomarenko, *supra* note 19, at 1832. Accordingly, they suggest, "judicial review ought to be directed at ensuring that policing is based ex ante on democratically founded rules." *Id.*

282. Eric Miller similarly writes that "police rulemaking is most often not open to public input," which, accordingly, limits public participation. Eric J. Miller, *Challenging Police Discretion*, 58 HOW. L.J. 521, 522–23 (2015).

283. Paul Ohm therefore advocates for "*intra-agency* separations of powers" as regards federal surveillance. Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 271 (2012).

284. *See* Susan W. Brenner, *The Voice of the Community: A Case for Grand Jury Independence*, 3 VA. J. SOC. POL'Y & L. 67, 86–87 (1995) (explaining that, without a court order, all evidence presented to a grand jury may only be shared with prosecution teams and other grand juries).

285. *See, e.g.*, Joseph Cox, *Pentagon Surveilling Americans Without a Warrant, Senator Reveals*, VICE (May 13, 2021, 1:00 PM) https://www.vice.com/en/article/88ng8x/pentagon-americans-surveillance-without-warrant-internet-browsing [https://perma.cc/KU2P-HRVG] (exploring possible warrantless surveillance of Americans by the U.S. Department of Defense).

286. Rozenshtein, *supra* note 20, at 146–47 (discussing ways in which providers offer transparency into government data requests). One exception to this may be the annual reporting required of the Department of Justice under the Wiretap Act. 18 U.S.C. § 2519.

only in the context of individual criminal cases.[287] As a result, the associated process "costs" of executive branch surveillance arise well after the fact.

In contrast, Congress is a process-heavy institution,[288] and, importantly, a democratically accountable one.[289] As such, congressional decision making tends to be both transparent and permeable. Actors external to Congress, both public and private, can have significant insight into and impact on Congress's choices.[290] This transparency and accountability creates a different dynamic for Congress than the executive, and it may help to ensure that Congress exercises self-restraint—choosing to engage in surveillance only when the benefits outweigh the procedural (and political) costs.[291]

I do not claim here that Congress's current process limits are sufficient, or that alternative processes would not be advisable. But I

---

287. Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 636–37 (2018) (arguing that the consequence of ex-post notice requirements for government hacking is that "the government can hack with no transparency until it elects to subpoena a particular hacked user's ISP for subscriber information and identifies the user through further investigation").

288. *See, e.g.*, Jonathan S. Gould, *Law Within Congress*, 129 YALE L.J. 1946 *passim* (2020) (focusing on how "parliamentary precedent" takes on qualities of law); Primus, *supra* note 28, at 587 ("The foremost strategy [for controlling congressional power] was that of process limits, which is to say that the whole structure of power and office-holding that the Constitution created is properly understood as a set of devices for constraining the federal government as well as empowering it.").

289. Voters can choose to remove members who exercise authority in ways they do not support. As case in point, every midterm election over the past 20 years has resulted in a change in party control in at least one chamber. Scott Bomboy, *How Midterm Elections Have Changed Congress Since 1946*, NAT'L CONST. CTR.: CONST. DAILY (Nov. 6, 2018), https://constitutioncenter.org/blog/how-midterm-elections-have-changed-congress-since-1946 [https://perma.cc/SUC5-JDTH] (examining the history of U.S. midterm federal elections since 1946 and noting their tendency to shift partisan control of at least one congressional legislative chamber); *see also* Jonathan Martin & Alexander Burns, *Democrats Capture Control of House; G.O.P. Holds Senate*, N.Y. TIMES (Nov. 6, 2018), https://www.nytimes.com/2018/11/06/us/politics/midterm-elections-results.html [https://perma.cc/FDM8-48E4] (announcing that the 2018 midterm elections changed the party controlling the House).

290. These actors include the executive branch, voters, state and local officials, the private sector, and even foreign governments. *See* Aziz Z. Huq & Jon D. Michaels, *The Cycles of Separation-of-Powers Jurisprudence*, 126 YALE L.J. 346, 391, 403–06 (2016) (cataloguing the "thick political surround" of actors external to the executive and legislative branches).

291. Friedman and Ponomarenko argue in favor of process limits to constrain law enforcement surveillance practices as an exercise of democratic accountability. *See* Friedman & Ponomarenko, *supra* note 19, at 1891–1903.

do contend that the weak external and internal limits on Congress's investigative authorities should not be viewed in isolation; rather, we should consider them in tandem with the political and procedural considerations that give rise to (or in some cases, might stymie) Congress's surveillance decisions.

2. The process of congressional surveillance

The process limits on congressional surveillance derive principally from the subpoena enforcement mechanism. Issuing a subpoena is rarely the first step for a committee. But, in the world of government surveillance, voluntary disclosures are the exception rather than the rule; providers may insist on a subpoena even if they intend to comply with a committee's demand.[292]

There are few costs to the way in which committees initially authorize subpoenas. In fact, the typical requirements for a committee to issue a subpoena are somewhat perfunctory, and observers are probably correct that the ease with which committees can subpoena does little to constrain them.[293] For instance, the process does not always require public debate, bipartisanship, or other significant up-front costs.[294] Rather, most congressional committees now have the authority to issue subpoenas independently of their chamber, and for some, the chair (either jointly with or after noticing the ranking member) may authorize a subpoena even without a committee vote.[295] Recently, Senate committees have also voted to grant the chair broad authority to issue multiple subpoenas, rather than requiring committee votes on each one.[296]

---

292. *See supra* Section II.A.1.b.ii.

293. *See* Marshall, *supra* note 57, at 803–04 (explaining that committees and committee chairmen can often unilaterally exercise the power to issue subpoenas without outside authorization at virtually no cost to Congress or the committee).

294. *See id.* at 805–06 (discussing Congress's newfound reliance on standing committees to conduct investigations and issue subpoenas instead of the chamber as a whole).

295. *See* MICHAEL L. KOEMPEL, CONG. RSCH. SERV., R44247, A SURVEY OF HOUSE AND SENATE COMMITTEE RULES ON SUBPOENAS 1–2, 4–5, 11 (2018) (documenting chamber and committee subpoena rules).

296. *See, e.g.*, Nicholas Fandos, *Republicans Secure More Subpoena Power in Push to Discredit Russia Inquiry*, N.Y. TIMES (June 11, 2020), https://www.nytimes.com/2020/06/11/us/politics/republicans-subpoena-russia-inquiry.html [https://perma.cc/SNX2-HA8E] (discussing recent procedures approved in Senate committees expanding the reach of committee chairmen to unilaterally subpoena multiple documents and testimony).

In addition, subpoenas are often written in broad language, with the expectation that the terms of compliance may be negotiated with the recipient at a later date.[297] The standard legal requirements for a facially valid subpoena are similarly easy to satisfy. A committee need only authorize a subpoena pursuant to its rules, within its jurisdiction, and pertinent to the matter under investigation.[298] Finally, committees can issue subpoenas without any need or interest in enforcement but solely to make a political point.[299]

This process is not inherently problematic from the perspective of congressional access to private information. Suppose that the recipient of a subpoena is unlikely to resist compliance, or the committee has no interest in pursuing enforcement. In that case, the choice to issue a subpoena ultimately does not meaningfully alter the committee's access to information.[300] Instead, the decision to issue a subpoena reflects a different type of activity—one concerned with shaping public perception.[301] But a committee that issues a surveillance subpoena is likely interested in acquiring information for an investigative purpose—or at least, I will assume that to be the case for the purpose

297. For example, with subpoenas seeking documents from the executive branch, the parties typically follow an "accommodations" process intended to permit both Congress and the executive branch to resolve the information dispute while simultaneously fulfilling each party's respective constitutional needs. United States v. AT&T, 567 F.2d 121, 127 (D.C. Cir. 1977).

298. Wilkinson v. United States, 365 U.S. 399, 408–09 (1961). The additional requirements based on the subject's civil liberties, including the due process right to be sufficiently notified of the investigation's purpose and Fourth or First Amendment limits are properly understood as *external* limits, not procedural ones.

299. That is sometimes how congressional subpoenas are perceived even when they are intended to produce information. *See, e.g.*, Chafetz, *supra* note 267, at 530–33 (describing reactions to House subpoena for testimony by Special Counsel Mueller).

300. For example, a committee may choose to use its compulsory power to send a public message about the nature of its engagements or the witness—to connote an adversarial posture or the witness's actual or anticipated hostility—even if the witness would otherwise appear absent the subpoena. On occasion, the subpoena serves a useful purpose for the recipient as well, whether to convey publicly the witness's opposition to the committee's investigation or because a subpoena offers certain legal protections.

301. Chafetz calls this "overspeech." Chafetz, *supra* note 267, at 536. *See, e.g.*, Josh Gerstein, *Clinton Lawyer Rejects Subpoena for Current Server Security Details*, POLITICO (Sept. 23, 2016, 10:12 PM), https://www.politico.com/blogs/under-the-radar/2016/09/hillary-clinton-emails-subpoena-server-security-228614 [https://perma.cc/BF6P-NXC6] (quoting House Oversight Committee chairman's statement following notification from Secretary Hillary Clinton's attorney that she would not be providing all information requested in committee's subpoena).

of considering how the process might constrain congressional surveillance.[302] Therefore, it is the enforcement process that serves as the primary limiting factor.

Congress may pursue compliance with its subpoenas in three ways: (1) civil enforcement proceedings in federal court, (2) criminal contempt referrals to the Department of Justice, and (3) contempt of Congress (also known as inherent contempt).[303] My focus here is on the civil enforcement mechanism. This is in part because congressional committees rarely cite subpoena targets with inherent contempt.[304] At the same time, Congress is disincentivized from pursuing criminal contempt charges, because it must entrust the executive branch to vindicate its authority.[305] Indeed, the Department of Justice does not reflexively prosecute Congress's contempt referrals but rather exercises prosecutorial discretion.[306] By comparison, in a civil enforcement proceeding, Congress must persuade a judge to order compliance (and therefore still relies on another branch), but it may still advocate its own position.[307] Further, the two contempt mechanisms carry punitive sanctions, but civil enforcement offers a

302. I do not mean to diminish the potential that a committee could use, or threaten to use, a subpoena as a form of witness intimidation or harassment, but my argument focuses on congressional access to information.

303. *See* GARVEY, *supra* note 66, at 1.

304. *See, e.g.*, *id.* at 12 (describing the challenges of using inherent contempt, including time limits and perception as "unseemly," and noting that "the inherent contempt process has not been used by either body [House or Senate] since 1935").

305. *See* CHAFETZ, *supra* note 22, at 175, 190 (discussing the separation of powers consequences of Congress's contempt options).

306. As a result, the U.S. Attorney's Office for the District of Columbia, which is jurisdictionally responsible for criminal contempt referrals, has recently declined referrals for the prosecution of executive branch witnesses. *See, e.g.*, *No Criminal Prosecution of Holder for Contempt*, CNN (July 6, 2012, 9:23 AM), https://www.cnn.com/2012/06/29/politics/holder-contempt/index.html [https://perma.cc/B3VB-N9HZ] (discussing DOJ's decision to not pursue criminal charges for former Attorney General Eric Holder's contempt of Congress); Whether the Department of Justice May Prosecute White House Officials for Contempt of Congress, 32 Op. O.L.C. 65, 67 (2008) (opining that DOJ may not prosecute White House officials Harriet Miers or Joshua Bolten for declining to comply with a congressional subpoena based on the President's invocation of executive privilege).

307. *See* GARVEY, *supra* note 66, at 22 (explaining that civil enforcement requires a Congressional entity file suit in federal district court seeking judicial declaration of compliance).

judicial remedy to extract the desired information, which is more relevant here.[308]

Importantly, the costs associated with enforcing subpoenas against powerful service providers create significant transaction costs for committees contemplating poorly conceived requests. A subpoena is only as good as the ability to enforce it; as those enforcement costs rise, the likelihood of enforcement—and therefore the use of surveillance subpoenas—will presumably fall.[309]

These costs can arise in several ways. *First*, some checks exist because of the power of service providers, a lesson that has been illustrated in the standard government surveillance context.[310] Congressional surveillance involves seeking information from a legally sophisticated entity, possibly one of the most profitable and powerful companies in the world. Whether one considers them to be "surveillance intermediaries"[311] or "Digital Switzerlands,"[312] these entities can create significant checks on government demands for data through a variety of actions, including public transparency, litigation, lobbying, and technological mechanisms.[313] Service providers are increasingly incentivized to resist subpoena demands by a user base and society that values privacy and may be suspicious of a transparently partisan demand.[314] As a result, the power and role of the subpoena recipient create a potential check.

In disputes with service providers, Congress lacks the alternative enforcement mechanisms that are typically available in disputes with

---

308. As the Congressional Research Service has observed, "Unlike criminal contempt, in a civil enforcement, sanctions (imprisonment and/or a fine) can be imposed until the subpoenaed party agrees to comply thereby creating an incentive for compliance; namely, the termination of punishment." *Id.* at 24.

309. I assume here that the purpose of enforcing a subpoena is to obtain information, and not to make a political point. This seems to be a safe assumption for surveillance subpoenas, which rarely have the same public impact as, for example, a subpoena for a President's tape recordings, and in my view, create incentives that support non-compliance. When a subpoena is directed towards largely political ends, the power of contempt—either inherent or criminal—is likely more appealing.

310. *See* discussion *supra* Section II.A.2.a-b.

311. Rozenshtein, *supra* note 20, at 112.

312. Eichensehr, *supra* note 20, at 685.

313. Rozenshtein, *supra* note 20, at 122 (describing "techniques of resistance"); SCHNEIER, *supra* note 39, at 207 (describing options for private sector entities to oppose government surveillance).

314. *See, e.g.*, *Developments in the Law—More Data, More Problems*, 131 HARV. L. REV. 1714, 1729–36 (2018) (discussing incentives and disincentives to intermediary compliance with Congressional subpoenas and various instances of noncompliance).

the executive. For instance, Congress cannot stall appointments at a private company; decline appropriations for a service provider; or impeach its chief executive officer, all mechanisms through which Congress can force disclosure without initiating adversarial proceedings.[315] Congress certainly has the ability to legislate or even haul in a company representative for a public hearing.[316] However, legislative regulation of technology companies has proven anything but straightforward, and companies might find resistance tolerable (or even advantageous) depending on the circumstances. In such a stand-off, a resolution might ultimately depend on public perceptions of which party is the aggrieved and which is the aggressor.[317]

Second, the public nature of a congressional subpoena creates costs in the form of public opinion. Congressional subpoenas are not issued in secret, and Congress does not have the legal authority to gag providers from disclosing such requests, no matter how sensitive they may appear. By comparison, such non-disclosure orders are standard in the law enforcement context.[318] As a result, providers are able to disclose a potentially overbroad or abusive request to the public, as well as the subject. Providers can use disclosure to sway public opinion against enforcement. At a time when government surveillance tends to attract highly negative publicity, the consequence of a public fight might not be one that a committee would wish to pursue absent good cause.

The power of public disclosure is particularly forceful because Congress's authority relies in significant part on public perceptions of its legitimacy.[319] A Congress that abuses its authorities runs the risk of

---

315. *See, e.g.*, CHAFETZ, *supra* note 22, at 193–94 (reviewing the powers that Congress normally exercises to thwart executive branch contemnors' efforts to withhold information).

316. *See, e.g.*, KOEMPEL, *supra* note 296, at 4, 11 (discussing House and Senate committee authority to issue subpoenas).

317. For example, until July 2020, Jeff Bezos and Amazon had long resisted congressional calls for testimony. *See* David McCabe, *Amazon Says Jeff Bezos Is Willing to Testify Before Congress*, N.Y. TIMES (July 29, 2020), https://www.nytimes.com/2020/06/15/technology/amazon-jeff-bezos-congress.html [https://perma.cc/3FAP-M8ED]. The decision for Bezos to testify seemed responsive to changes in public perceptions of Amazon during the COVID-19 pandemic.

318. *See* 18 U.S.C. § 2705(b) (establishing process for a governmental entity to obtain a non-disclosure order).

319. As Chafetz argues, "[c]ongressional authority at any particular historical moment is in part a function of the success or failure of Congress's public engagements in past historical moments and in part a function of how adroitly

losing the political goodwill on which it heavily relies. Following the excesses of the McCarthy era, Congress visibly retreated from McCarthy's abuse of Congress's investigative powers.[320] Echoes of this self-moderation are observable in other ways in which Congress, as a matter of practice, abides by "unwritten rules of restraint."[321] For example, Congress tends to observe attorney-client privilege, even though nothing requires it to do so.[322]

I do not want to place too heavy a reliance on norms (for obvious reasons), but the point is that notions of legitimacy have an important and, at times, overriding force on Congress. If we think about aggressive uses of congressional surveillance as a norm-breaking form of "constitutional hardball," such actions may engender a tit-for-tat response when party control shifts.[323] This dynamic provides one possible explanation for Republicans' reluctance to engage in congressional surveillance against Congressman Schiff during the impeachment proceedings for President Trump. In this way, the

---

congressional members and leaders make use of historical reservoirs of authority in the present." CHAFETZ, *supra* note 22, at 314–15.

320. *See, e.g.*, HAMILTON, *supra* note 40, at 8–9 (commenting on reactions to the McCarthy-era "loyalty" investigations); Chafetz, *supra* note 267, at 595 (describing how the Watkins Committee, which handled the censure case of former Senator Joseph McCarthy, "would perform calmness and solemnity as a form of rebuttal" to McCarthy).

321. John C. Yoo, *Lawyers in Congress*, *in* CONGRESS AND THE CONSTITUTION 131, 145 (Neal Devins & Keith E. Whittington eds., 2005). Yoo describes, for example, the 1996 Judiciary Committee investigation of the Clinton administration's handling of FBI investigative files, in which letters "were framed very much like discovery requests in federal civil litigation" and "[c]laims of privilege were accepted if a proper explanation was provided." *Id.*

322. Michael D. Bopp & DeLisa Lay, *The Availability of Common Law Privileges for Witnesses in Congressional Investigations*, 35 HARV. J.L. & PUB. POL'Y 897, 907 (2012).

323. *See* Mark Tushnet, *Constitutional Hardball*, 37 J. MARSHALL L. REV. 523, 523 (2004) (defining constitutional hardball as "political claims and practices . . . that are without much question within the bounds of existing constitutional doctrine and practice but that are nonetheless in some tension with existing *pre*-constitutional understandings"). There are some differences of opinion as to whether one party or another engages more often in constitutional hardball. *Compare* Joseph Fishkin & David E. Pozen, *Asymmetric Constitutional Hardball*, 118 COLUM. L. REV. 915, 918 (2018) (arguing that "Republican officials have been more willing than Democratic officials to play constitutional hardball"), *with* David E. Bernstein, Response, *Constitutional Hardball Yes, Asymmetric Not So Much*, 118 COLUM. L. REV. ONLINE 207, 208, 212–16 (2018) (rejecting Fishkin and Pozen's assertion that constitutional hardball is entirely asymmetric, highlighting instances of Democratic constitutional hardball).

"separation of parties" might discourage the perceived norm-violating use of surveillance authorities.[324]

Third, there are procedural checks *within* Congress that might stave off improper surveillance activities. Perhaps most importantly, there are significant transaction costs to pursuing a subpoena enforcement action, even before it ever reaches court. On the Senate side, for example, committees do not have independent litigating authority under the Senate's enforcement statutes.[325] Rather, a committee must approve and send a resolution to the floor, at which point it must secure a majority vote of the full chamber to authorize civil enforcement.[326] And before any of that can happen, committee rules may require an opportunity for the witness to explain the objection and for the committee to rule on it.[327] Since 1979, the Senate has only authorized civil enforcement six times.[328] On the House side, the chamber can authorize its committees to pursue enforcement actions

---

324. According to the "separation of parties" theory advanced by Daryl Levinson and Richard Pildes, we might expect less congressional surveillance in a united government, and more in a divided government. *See* Daryl J. Levinson & Richard H. Pildes, *Separation of Parties, Not Powers*, 119 HARV. L. REV. 2311, 2338–47 (2006) (contending that competition between political parties drives interbranch dynamics). Nevertheless, party affiliation does not erase institutional allegiance entirely; CHAFETZ, *supra* note 22, at 29–33 (arguing that members sometimes align themselves with chamber over party); *see also, e.g.*, Seung Min Kim & Karoun Demirjian, *Decision to Subpoena Donald Trump Jr. Sets Off a Republican Firefight*, WASH. POST (May 9, 2019, 9:56 PM), https://www.washingtonpost.com/politics/decision-to-subpoena-donald-trump-jr-sets-off-a-republican-firefight/2019/05/09/cb3e8d3e-7272-11e9-9f06-5fc2ee80027a_story.html [https://perma.cc/9ACW-WZ4T] (discussing intra-Republican dynamics on the Senate Intelligence Committee over decision to subpoena Donald Trump Jr.).

325. *See* 28 U.S.C. § 1365(e) ("A civil action commenced or prosecuted under this section, may not be authorized pursuant to the Standing Order of the Senate 'authorizing suits by Senate Committees' (S. Jour. 572, May 28, 1928)."); TODD GARVEY, CONG. RSCH. SERV. R45653, CONGRESSIONAL SUBPOENAS: ENFORCING EXECUTIVE BRANCH COMPLIANCE 5–6, 6 n.37 (2019) (explaining that, prior to the enactment of 28 U.S.C. § 1365, the Senate had given its committees the authority to bring lawsuits).

326. 2 U.S.C. § 288d; 28 U.S.C. § 1365.

327. KOEMPEL, *supra* note 296, at 12 (describing various committee procedures relating to witness objections).

328. GARVEY, *supra* note 326, at 25 & n.188 (citing S. Res. 502, 96th Cong. (1980) (enacted); S. Res. 293, 98th Cong. (1984) (enacted); S. Res. 162, 101st Cong. (1989) (enacted); S. Res. 153, 103d Cong. (1993) (enacted); S. Res. 199, 104th Cong. (1995) (enacted); S. Res. 377, 114th Cong. (2016) (enacted)).

although it lacks an enforcement statute.[329] These full-chamber processes may very well serve to limit any potential abuse of Congress's surveillance tools, simply because the political parties do not line up in a traditional way on government access to private data.[330] And even once Congress authorizes a suit, it can still take a lengthy period of time to resolve a case once it arrives in court—months if not years—not to mention an extensive appeals process if the case has precedential value.[331]

In fact, Congress may initiate an enforcement proceeding against a provider, only to find that its opponent is, in some cases, the White House.[332] This is because providers involved in potential disputes concerning presidential or executive branch information may want to avoid picking winners between two branches, preferring instead to be ordered to do so by a court.[333] *Mazars* illustrates how this might play out.[334] Rather than litigate the subpoenas, the financial companies asked the court to determine whether they were legally obligated to

---

329. Recent cases have concluded that the House may rely on general federal question jurisdiction. *See, e.g.*, Comm. on the Judiciary v. Miers, 558 F. Supp. 2d 53, 64 (D.D.C. 2008) (finding federal question jurisdiction under 28 U.S.C. § 1331 appropriate for an action seeking to enforce a congressional subpoena); Comm. on Oversight & Gov't Reform v. Holder, 979 F. Supp. 2d 1, 17 (D.D.C. 2013) (same); *see also* Reed v. Cnty. Comm'rs, 277 U.S. 376, 388–89 (1928) (holding that Senate committee was not authorized to sue to enforce a subpoena that had not been specifically authorized by Senate resolution).

330. *See, e.g.*, Jordain Carney, *Trump, Privacy Hawks Upend Surveillance Brawl*, HILL (Mar. 15, 2020, 8:00 AM), https://thehill.com/policy/national-security/487537-trump-privacy-hawks-upend-surveillance-brawl [https://perma.cc/Q26J-AY2W] (highlighting division within the GOP on surveillance legislation).

331. In an unusually expeditious ruling, it took only five months for the district court to rule on a subpoena in the Senate investigation of Backpage. *See* Senate Permanent Subcomm. on Investigations v. Ferrer, 199 F. Supp. 3d 125, 128 (D.D.C. 2016), *vacated as moot*, 856 F.3d 1080, 1089 (D.C. Cir. 2017). The timetable is typically longer in a suit against the executive branch. For example, the parties jointly agreed to dismiss *Miers* litigation pending a D.C. Circuit decision after nineteen months. Motion for Voluntary Dismissal by Plaintiff, Comm. on the Judiciary v. Miers, 558 F. Supp. 2d 53 (D.D.C. 2008) (No. 1:08-cv-00409) 2009 WL 5187074.

332. Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2027–28 (2020); *see also* TODD GARVEY, CONG. RSCH. SERV., LSB10517, TRUMP V. MAZARS: IMPLICATIONS FOR CONGRESSIONAL OVERSIGHT 2 (2020) (arguing that while the companies hold the relevant information, the "real dispute is between the President and the House committees").

333. *See Mazars*, 140 S. Ct. at 2028 ("Although named as defendants, Mazars and the banks took no positions on the legal issues in these cases").

334. *See id.*

comply, creating an opening for President Trump to contest the disclosure.[335] Many months later, the Court remanded the case for further consideration, effectively granting President Trump a victory and the House a defeat.[336]

Understanding enforcement is important because the mere possibility of litigation should theoretically give a congressional committee pause. Litigation is a time and resource intensive enterprise with uncertain outcomes. If Congress loses, it suffers a precedent-setting result, which could potentially stymie future enforcement efforts and undermine the legitimacy of a committee's requests in that same investigation. If Congress wins, it must survive a lengthy litigation process, which is especially daunting if litigation must occur repeatedly.[337] Accordingly, these process constraints create meaningful incentives for Congress to limit its demands.

III. *MAZARS* AND CONGRESSIONAL SURVEILLANCE

Taken collectively, the limits I described in Part II depend more on Congress's unique procedural and political constraints than on established statutory and Fourth Amendment mechanisms. But, as explained in Part I, congressional surveillance is stubbornly *congressional*, meaning that we should also account for how congressional surveillance implicates the separation of powers.[338] This Part builds on that notion, contending that congressional surveillance is not just "mere" surveillance, but is a valid tool within the separation of powers. When facing stalled inter-branch information disputes, Congress can use surveillance to advance investigations, countering

335. *Id.* at 2027–28.

336. *See* Josh Chafetz, *Don't Be Fooled, Trump Is a Winner in the Supreme Court Tax Case*, N.Y. TIMES (Jul 9, 2020), https://www.nytimes.com/2020/07/09/opinion/trump-taxes-supreme-court-.html [https://perma.cc/J9VC-3RQY]. Following the decision, the Court also rejected House requests to expedite its remand. *See* Pete Williams, *Supreme Court Rejects House Democrats' Plea to Speed Up Trump Tax Case*, NBC NEWS (July 20, 2020, 11:28 AM), https://www.nbcnews.com/politics/supreme-court/supreme-court-won-t-rush-trump-tax-fight-congress-lower-n1234348 [https://perma.cc/7FJP-G3P4].

337. The Senate Select Committee sued to obtain President Nixon's tapes, arguably the most important civil lawsuit to enforce a subpoena at that time, on August 9, 1973, approximately one month after the committee learned of the tapes. But it took so long to resolve, even on an expedited basis, that the court of appeals did not issue a final decision until May 23, 1974, only a month and a half before the committee ceased its investigations. HAMILTON, *supra* note 40, at 43.

338. *See supra* Part I.

the White House's increasing invocation of executive privilege. And congressional surveillance can empower Congress to engage in digital governance rather than ceding that terrain to technology companies.

In *Mazars*, the Supreme Court treated this new dynamic as a separation of powers *concern*, rather than a separation of powers *benefit*.[339] In failing to address the background privacy threat posed by congressional surveillance of personal information, the Court erroneously focuses on concerns regarding the separation of powers.[340] In doing so, *Mazars* gets it backwards, and its decision is both over- and under-inclusive as to privacy. Instead, as this Article concludes, the treatment of congressional surveillance must account for case-by-case privacy interests while preserving Congress's ability to assert itself as a co-equal branch.

A. Surveillance and Separation of Powers

This Section defends congressional surveillance as an important component of Congress's Article I roles, in contrast to the skepticism exhibited in *Mazars*. First, there are legitimate benefits to Congress's role in checking the executive branch—benefits that offer it the potential to counter the expanding use of executive privileges and immunities. Second, there are tangible, practical benefits when Congress uses access to digital information to enhance digital governance. In this way, it is possible to think of congressional surveillance not as ordinary surveillance or even ordinary governance, but rather as a tool of Josh Chafetz's "constitutional politics"—the "meta-politics" of distributing authority among government institutions "to decide questions of collective self-government."[341]

1. Checks and balances

The growth of executive authority has come in significant part at Congress's expense, and Congress's inability to counter the executive has become as American as baseball and apple pie. Nowhere was this more apparent than the White House's stonewalling in response to the

---

339. *Mazars*, 140 S. Ct. at 2033–35 (finding that congressional subpoenas issued by the U.S. House of Representatives and served upon then-President Donald Trump in his personal capacity represented a "clash between rival branches of government").

340. *Id.* at 2034 (noting that "[t]he President is the only person who alone composes a branch of government," so "there is not always a clear line between his personal and official affairs").

341. CHAFETZ, *supra* note 22, at 16.

House's 2019 impeachment inquiry.[342] But these events also offer a compelling justification for Congress to turn to its surveillance authorities. In this view, congressional surveillance serves as a component of checks and balances, necessary to counter executive authority and maintain Congress's position as a co-equal branch. To understand why, it is helpful to consider the dynamic between Congress and the executive branch, which suggests that congressional surveillance is not simply a political act but also represents a legitimate separation of powers tool.

Congress's ability to conduct investigations concerning the President and other executive branch actors has always been a balance between the demonstrated need of the legislature and the various government privileges that the executive can assert.[343] Chafetz and others have examined the ways in which Congress and the executive branch use various tools in inter-branch information and oversight disputes.[344] For example, Congress can subpoena information or testimony from a cabinet member backed by contempt,[345] withhold (or fence) appropriations until certain actions are taken,[346] and the Senate can hold up nominations until its disclosure demands are met.[347]

---

342. *See* Amber Phillips, *The White House Has Stonewalled Impeachment. How Will Congress Proceed?*, WASH. POST (Oct. 9, 2019, 4:23 PM), https://www.washingtonpost.com/politics/2019/10/09/white-house-has-stonewalled-impeachment-how-will-congress-proceed [https://perma.cc/QX6F-NBPY] (discussing the White House's statement that it would not cooperate with Congress's impeachment inquiry).

343. *See* TODD GARVEY & DANIEL J. SHEFFNER, CONG. RSCH. SERV., R45442, CONGRESS'S AUTHORITY TO INFLUENCE AND CONTROL EXECUTIVE BRANCH AGENCIES 34–35 (2021) (discussing Congress's investigatory powers as an implicit legislative power and the executive's various privilege assertions in response).

344. *See, e.g.*, CHAFETZ, *supra* note 57, at 715–16 (discussing various tools that Congress "can deploy in interbranch conflicts").

345. *Id.* at 735–38.

346. *Id.* at 734–35, 738.

347. *See, e.g.*, *id.* at 738. Practice suggests that there need not be a link between the nomination and the disclosure request. For example, Senator Grassley held up the nomination of William Evanina to be Director of the National Counterintelligence and Security Center over the Department of Justice's failure to respond to document requests. *See* Martin Matishak, *After Nearly 2 Years, Grassley Lifts Hold on Counterintel Chief Nominee*, POLITICO (May 5, 2020, 8:59 AM), https://www.politico.com/news/2020/05/04/grassley-national-counterintelligence-235342 [https://perma.cc/9ADB-GEYU] (explaining how Senator Grassley delayed the nomination of President Trump's pick for the country's new counterintelligence chief while he waited for Congress to surrender documents related to Trump's nomination, citing congressional oversight as a power that the executive branch needs to respect).

In response to Congress's demands for information, the executive branch tends to assert various forms of executive privilege relating to deliberative process, national security interests, foreign affairs and diplomacy, and the confidentiality of presidential communications and those of the President's senior advisors.[348] Under this privilege umbrella, the executive branch may seek to limit its disclosures, disclose information only as confidentiality interests fade, or decline to disclose any information at all.[349] The use of executive privilege claims to withhold information from Congress is a practice that has surfaced in practically every significant information dispute in recent memory.[350]

Increasingly, as Jonathan Shaub has observed, the privilege has taken on a "prophylactic" role.[351] That is, the executive branch does not assert privilege *after* it concludes that the harms from disclosure outweigh Congress's interest in the information, but rather to preserve *in advance* the President's ability to make that determination in the first place.[352] As a result, the executive branch can decline to disclose information in response to legitimate congressional requests without ever actually asserting the privilege.[353] This practice is in addition to claims of absolute immunity that the executive has sought to extend to

---

348. For a primer on executive privilege and the related accommodations process, see generally John E. Bies, *Primer on Executive Privilege and the Executive Branch Approach to Congressional Oversight*, LAWFARE (June 16, 2017, 8:30 AM), https://www.lawfareblog.com/primer-executive-privilege-and-executive-branch-approach-congressional-oversight [https://perma.cc/HU57-LWED] (defining executive privilege, how it can be asserted, and limitations of the power).

349. *Id.*

350. There have been some ebbs and flows over time. *See generally* MARK J. ROZELL WITH MITCHEL A. SOLLENBERGER, EXECUTIVE PRIVILEGE: PRESIDENTIAL POWER, SECRECY, AND ACCOUNTABILITY ix–x (4th ed. 2020) (discussing how every President from Bill Clinton on has used executive privilege to withhold information).

351. *See* Shaub, *supra* note 35, at 7–8.

352. *Id.* at 27–28.

353. Congressional hearings relating to Russian interference during the 2016 election surfaced some interesting applications of this phenomenon, such as a presidential transition advisor declining to answer questions about activities during the transition to preserve the President's ability to assert privilege. *See* Andy Wright, *On Bannon's Testimony and Executive Privilege*, JUST SEC. (Jan. 18, 2018), https://www.justsecurity.org/51134/bannons-testimony-executive-privilege [https://perma.cc/C9YH-WQX9] (detailing how presidential transition advisor declined to answer questions from congressional committee by arguing his answers could intrude on the President's sole authority to determine whether or not to assert executive privilege).

senior White House advisors.[354] Some have suggested that this dynamic threatens to render Congress largely ineffective in oversight disputes, and it is not hard to see why.[355]

To obtain information in these circumstances, Congress is often forced to the negotiating table. In 1976, for example, the House Committee on Interstate and Foreign Commerce subpoenaed documents from the Ford administration relating to FBI electronic surveillance practices using AT&T facilities.[356] President Ford offered a limited set of disclosures in the way of a compromise, which the House rejected and followed with a subpoena to AT&T for national security letters issued by the Department of Justice.[357] In response, the Department of Justice obtained an injunction against AT&T's compliance, on the basis that disclosure of such information would jeopardize national security interests if made public, and that AT&T was serving as an "agent" of the government.[358] The House appealed.[359] But rather than impose its own judgment on the parties—a "delicate problem of accommodating the needs and powers of two coordinate branches in a situation where each claimed absolute authority"—the D.C. Circuit ordered the parties to engage in an accommodations process, in which each branch should recognize "an implicit constitutional mandate to seek optimal accommodation through a realistic evaluation of the needs of the conflicting branches."[360]

In effect, the decision sent the parties right back to where they started, and this directive to engage in accommodations has aided the executive branch in invoking privilege while preventing Congress from

---

354. Adam Liptak, *In McGahn Case, an Epic Constitutional Showdown*, N.Y. TIMES (May 24, 2021), https://www.nytimes.com/2020/01/13/us/politics/mcgahn-trump-congress-lawsuit.html [https://perma.cc/KJ25-MMX2] (discussing President Trump's contention that his senior aides have absolute immunity).

355. In reaction, Shaub suggests that executive privilege should only be understood as a "limited presidential immunity from compelled congressional process," thereby preventing its use in other forms of oversight. Shaub, *supra* note 35, at 2, 61.

356. ROZELL WITH SOLLENBERGER, *supra* note 350, at 82 (highlighting an example of when a congressional committee required information being withheld by the President to conduct an investigation of wiretapping activity).

357. United States v. Am. Tel. & Tel. Co. (*AT&T II*), 567 F.2d 121, 122–23 (D.C. Cir. 1977); United States v. Am. Tel. & Tel. Co. (*AT&T I*), 551 F.2d 384, 385–86 (D.C. Cir. 1976).

358. *AT&T I*, 551 F.2d at 387.

359. *AT&T II*, 567 F.2d at 123.

360. *Id.* at 123, 127.

promptly obtaining compliance.[361] This is because the two parties are not similarly situated if they choose to negotiate. Most importantly, the executive branch holds the information, and Congress does not. This means that Congress must act in order to prevail, but the executive branch can protect its position by simply doing nothing at all.[362] But, in addition, the time horizons for each branch are different, such that the executive branch can engage in delay tactics that can take years, whereas both chambers of Congress undergo elections every two years that may result in a change of party control and a corresponding shift in the chamber's interest in compliance. Negotiations, especially if there are multiple iterations of requests, can eat into time that one of the parties simply does not have.[363] Finally, the executive branch takes a unitary approach to its position on privilege and the manner in which it negotiates. Disclosures are governed by presidential memoranda and, when they concern potentially privileged information, are typically vetted by the Office of Legal Counsel and the White House.[364] By comparison, congressional committees and each chamber can act independently of one another, without a formalized, uniform view, especially when they are controlled by different parties.[365]

Theoretically, however, the executive's privileges are available only when the executive is the recipient of a request for information that it controls: in other words, when it has maintained confidentiality over the records.[366] Disclosure outside the privileged circle should generally

---

361. The accommodations process is now effectively required by statute because courts lack jurisdiction to resolve a compliance dispute between the Senate and a government official asserting a government privilege. 28 U.S.C. § 1365.

362. *See, e.g.*, Ashley Deeks, *Checks and Balances from Abroad*, 83 U. CHI. L. REV. 65, 65, 69–71 (2016) (noting the deleterious effect on oversight when "[t]he executive possesses significant informational and operational advantages").

363. *See, e.g.*, Chafetz, *supra* note 57, at 738–40 (noting the timing of resolution in the Miers and Bolten contempt disputes); Neal Devins, *Congressional-Executive Information Access Disputes: A Modest Proposal—Do Nothing*, 48 ADMIN. L. REV. 109, 126 (1996) (noting that "[d]ispute resolutions can eat up a great deal of staff resources (from both sides) and can take several months").

364. Shaub, *supra* note 35, at 31.

365. *See* Chafetz, *supra* note 22, at 38 ("Congress is frequently hampered by its internal divisions.").

366. Shaub, *supra* note 35, at 32–34. Confidentiality in this regard is treated more narrowly than evidentiary privileges, as "the executive branch has typically understood the disclosure of information regarding agency deliberations or classified information to waive protection only of the specific information disclosed or officially acknowledged." Bies, *supra* note 349 (discussing the legal and prudential

eliminate the privilege.[367] For instance, Presidents cannot assert executive privilege over financial records held by their banks.[368] By the same token, the White House could not prevail on a claim of executive privilege over phone records held at a private telephone provider for calls that the President has placed on a personal cell phone, especially if those calls took place before taking office.[369] Additionally, the White House could not assert executive privilege over the phone records, location information, or communications of an associate of the President who is not an executive branch official at all.

With its surveillance requests, like any other request to private entities, Congress can capitalize on these limits and circumvent the tools that the executive normally uses to slow or disrupt Congress's work. In other words, rather than engage in protracted and increasingly fruitless inter-branch negotiations, congressional committees can opt instead to gather information directly from the hands of service providers.[370] This strategy is available because a small number of communications service providers maintain the available user data—the Facebooks, Twitters, Googles, Apples, and Amazons of the world—and not a government agency or the individuals themselves.[371] As described in Part I, the information available to Congress through these providers may outstrip even the information the executive branch could provide.[372]

The House's 2019 impeachment subpoenas to telephone providers AT&T and Verizon illustrate this dynamic. The House obtained records that revealed phone calls between Igor Fruman, who had been

considerations the attorney general and White House counsel must weigh before recommending executive privilege).

367. Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2032–33 (2020).

368. For that reason, Trump did not assert such a privilege in the *Mazars* litigation, although he sought the equivalent protection. *Id.* at 2028–29.

369. I do not mean to suggest that the White House in such circumstances would not make such an argument or would otherwise lack a basis to contest the request. However, the argument it would make is not based on a privilege against disclosures, but rather an internal limits argument, discussed *infra*, about whether Congress's power would appropriately reach that information in the first place.

370. *See supra*, notes 316–38 and accompanying text.

371. *See* Carly Miller, *Can Congress Mandate Meaningful Transparency for Tech Platforms?*, BROOKINGS: TECH STREAM (June 1, 2021), https://www.brookings.edu/techstream/can-congress-mandate-meaningful-transparency-for-tech-platforms [https://perma.cc/2VDY-6TXU] (providing an illustration of the type of data that providers such as Facebook possess, and the lack of Congressional control currently imposed).

372. *See supra* Part I.

involved in arranging the Ukraine deal, Congressman Devin Nunes, journalist John Solomon, and President Trump's personal lawyer, Rudy Giuliani.[373] U.S. Ambassador Gordon Sondland was also a subject of a phone records subpoena.[374] It is unlikely that these individuals would have produced the requested records if the HPSCI had asked them directly. Indeed, as described in the HPSCI report, "[a] subpoena served to the White House requesting certain call records was obstructed in full by President Trump."[375] *Mazars* illustrates the same dynamic, where congressional investigators pursued the President's financial records and tax return information through requests to third-party entities, and not the President himself.[376]

To be sure, this is not a panacea. Historical precedent and current disputes suggest that the executive branch will nonetheless seek to intervene in such requests, at least when it is put on notice and retains a plausible interest in maintaining confidentiality.[377] Regardless, my argument is not that Congress is or is not *entitled* to certain information, but rather that its decision to *pursue* that information from a third party responds to executive branch maneuvers and should be considered through that lens. In other words, at the core of congressional surveillance is a conflict between the executive and legislative branches about *who* decides Congress's investigative legitimacy. From this perspective, Congress's exercise of surveillance

373. *See* HPSCI Report, *supra* note 3, at 43, 45–46, 46 n.49.

374. Wong & Brufke, *supra* note 3.

375. HPSCI Report, *supra* note 3, at 153 n.49. At the time, the President had directed the federal government not to cooperate with any requests from the House—a directive that, from Congress's perspective, arrogated to the White House the decision of what and was not a legitimate oversight purpose and formed the basis for one article of impeachment. *See* Articles of Impeachment Against Donald John Trump, H. Res. 755, 116th Cong., art. II (2019) ("President Trump sought to arrogate to himself the right to determine the propriety, scope, and nature of an impeachment inquiry . . . as well as the unilateral prerogative to deny any and all information to the House of Representatives in the exercise of its 'sole Power of Impeachment.'").

376. As the House noted at oral argument, not only did its request cover information that was in the control of a private entity, but also included information that the President himself had never seen and was not even aware of. *See* Transcript of Oral Argument at 69, Trump v. Mazars USA, LLP, 104 S. Ct. 2019 (2020) (No. 19-715).

377. *See* Kirsten Carlson, *Courts Have Avoided Refereeing Between Congress and the President, but Trump May Force Them to Wade In*, THE CONVERSATION (Dec. 6, 2019, 10:59 AM), https://theconversation.com/courts-have-avoided-refereeing-between-congress-and-the-president-but-trump-may-force-them-to-wade-in-128269 [https://perma.cc/5TNK-WEV7] (detailing instances of Presidents who have asserted executive privilege to defy congressional subpoenas).

authorities operates as a tool of "constitutional politics" because it represents a claim by Congress that it—and not the President—should decide the information that is relevant to its investigative priorities. And in doing so, it offers the benefit of restoring to Congress the ability to check presidential assertions of executive privilege and resistance to oversight.

2. Fact gathering and digital governance

There is also a far more mundane, but equally important reason, for Congress to value access to communications data. Digital information has become both more revealing and more important to Congress's oversight and legislative roles. Digital interactions are integral to public and private life, at times replacing entirely their physical analogs—a trend that has been exhaustively documented elsewhere.[378] For instance, letters have become emails and instant messages; photo albums are now on Instagram; we socialize on Facebook; and the bull horn is now Twitter.

But in addition, the problems requiring congressional attention are now, as often as not, centered on digital issues. Technology has come to dominate not just the ways in which we communicate in private, but also the ways in which we engage publicly in core democratic activities.[379] Whether it is examining the influence activities of Cambridge Analytica and the Russian Internet Research Agency (IRA),[380] the sex trafficking on Backpage.com,[381] the problem of

---

378. *See, e.g.*, Janice Denegri-Knott et al., *What is Digital Possession and How to Study It: A Conversation with Russell Belk, Rebecca Mardon, Giana M. Eckhardt, Varala Maraj, Will Odom, Massimo Airoldi, Alessandro Caliandro, Mike Molesworth and Alessandro Gandini*, 36 J. OF MKTG. MGMT. 942, 948 (2020) (discussing the shift from physical to digital possessions).

379. *See, e.g.*, Abby Hay, *Social Media Increases Civic Engagement Among Users*, DAILY UNIVERSE (Aug. 30, 2016), https://universe.byu.edu/2016/08/30/social-media-increases-civic-engagement-among-users [https://perma.cc/8RWR-X2C7] (discussing how social media affects civic engagement).

380. Sean Illing, *Cambridge Analytica, the Shady Data Firm that Might Be a Key Trump-Russia Link, Explained*, VOX (Apr 4, 2018, 3:41 PM), https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie [https://perma.cc/AL2M-MLDH] (discussing potential collusion with Russia).

381. Dustin Volz, *U.S. Senate Holds Backpage.com in Contempt over Sex Trafficking Ads*, REUTERS (Mar. 17, 2016, 3:30 PM), https://www.reuters.com/article/usa-congress-trafficking-idUSL2N16P1N4 [https://perma.cc/RN5M-2W2B] (stating that Backpage.com had engaged in sex trafficking for two decades).

encryption for child exploitation,[382] or potential reforms to section 230 of the Communications Decency Act,[383] there is a compelling argument that Congress cannot adequately understand or engage with today's pressing issues without doing its digital due diligence.

For example, the 2016 election influence activities of the Russian IRA presented more than just a law enforcement matter for the Special Counsel, although they eventually resulted in criminal charges.[384] They also posed fundamental questions for Congress's oversight and legislative mandates: how did Russian actors manipulate social media? How prevalent is foreign influence targeting Americans? What, if anything, could technology platforms have done to identify and mitigate those activities? What was the involvement of the political campaigns? Was legislation or regulation necessary, and if so, what should be done?[385] The ability for a congressional committee to answer these questions and others relies on its capacity to access and understand digital information in the hands of private technology companies. Likewise, as to Lev Parnas's cell phone—if those are the ways that witnesses use to communicate, then it makes perfect sense for Congress to apply forensic tools in analyzing the evidence.

Access to this sort of information also alleviates other oversight and investigative obstacles that Congress routinely encounters. Most significantly, Congress faces "information gathering" costs when conducting oversight. These costs are the byproduct of its reliance on the executive branch to provide information for oversight purposes, a lack of expertise in certain highly-specialized areas, and uncertainty surrounding the initial allocation of resources.[386] Recent scholarship

---

382. Stewart Baker, *The EARN IT Act Raises Good Questions About End-to-End Encryption*, LAWFARE (Feb. 11, 2020, 2:53 PM), https://www.lawfareblog.com/earn-it-act-raises-good-questions-about-end-end-encryption [https://perma.cc/5ZN5-PBCK] (discussing the effect of encryption on companies addressing child pornography).

383. 47 U.S.C. § 230 (2018).

384. The special counsel's office charged the IRA with conspiracy to defraud the United States, wire fraud, and aggravated identity theft. *See* Indictment, United States v. Internet Rsch. Agency, Crim. No. 1:18-cr-00032-DLF (Feb. 16, 2018).

385. *See, e.g.*, *Social Media Influence in the 2016 U.S. Election: Hearing Before the S. Select Comm. on Intel.*, 115th Cong. 1–3, 6 (2017) (statements of Sen. Burr, Chairman, S. Select Comm. On Intel. and Sen. Warner, Member, S. Select Comm. On Intel.).

386. Sarah A. Binder & Frances E. Lee, *Making Deals in Congress*, *in* NEGOTIATING AGREEMENT IN POLITICS 54, 59, 65 (Jane Mansbridge & Cathie Jo Martin eds., 2013) (explaining how Congress must consult with various outside groups to gather information to inform members on highly specialized legislation and negotiations); William P. Marshall, *Eleven Reasons Why Presidential Power Inevitably Expands and Why It*

has suggested, however, that in the digital space Congress can "piggyback[]" on the work of large communications service providers.[387] For example, providers can signal emerging issues worthy of congressional oversight, pulling the "fire alarm[]" for Congress's attention.[388]

Just as important, Congress's first-hand access to digital information can help decrease its oversight costs simply by virtue of the data's availability. For instance, a committee may well prefer to review one person's cell phone instead of conducting an interview, or to peruse data belonging to thousands of Facebook accounts rather than holding thousands of interviews (as if holding a thousand interviews could even be done).[389]

Collecting information independently from third parties might be more effective than relying on providers to analyze and report information themselves, especially if the committee's focus is to understand whether legislation of technology companies is necessary—a task obviously unsuitable for outsourcing to the companies themselves. Indeed, we might consider technology companies as another component of the separation of powers, one in which Congress must compete not only against the other branches, but also powerful private entities that it seeks to regulate. If we do, then congressional access to information held by those companies immediately resembles its disputes over access to information with the executive. Put differently, oversight of a powerful industry has important commonalities with oversight of the executive branch, including at the core a political tension over governance authority. To that point, congressional surveillance not only empowers Congress in

---

Matters, 88 B.U. L. REV. 505, 515–16 (2008) (detailing that Congress often must rely the executive branch for "information gathering capabilities" that is less accessible to congressional members and staff).

387. *See, e.g.*, Rozenshtein, *supra* note 20, at 151 (arguing that "[j]ust as surveillance intermediaries increase the benefits Congress gets from overseeing surveillance, they also decrease the costs Congress incurs for conducting such oversight"); Deeks, *supra* note 363, at 84 (noting that "technology firms help Congress overcome its informational disadvantages on technology and information about US intelligence-community operations").

388. Rozenshtein, *supra* note 20, at 151.

389. For example, the SSCI used the data that social media companies had disclosed and shared it with technical experts for analysis. This sort of independent auditing filled a capacity gap within the Committee, but also ensured that the Committee was not relying solely on the narrative or analysis developed by the providers themselves. *See* SSCI REPORT, *supra* note 1, at 73–74.

inter-branch dynamics, but also with respect to the private sector that it oversees.

B. Mazars *and Privacy*

I do not intend the above to be an exhaustive survey of the reasons that Congress has a growing institutional need to access digital information; there are certainly others. But what I do hope to illustrate is that Congress has legitimate reasons to pursue access to data, and that any discussion of a surveillance system design should account for those separation of powers benefits. At the same time, however, this Article has also demonstrated that congressional surveillance lacks the privacy protections that operate in other areas of government surveillance.[390]

Because it stands at the intersection of these two areas of law, congressional surveillance can be framed in two ways. It can be framed as a separation of powers issue, in which access to private information depends on the relative interests and rights of two co-equal branches. Or it can be framed as a privacy issue, in which access to private information depends on a balancing of government need and individual rights.

In *Mazars*, the Court opted in favor of the separation of powers model.[391] That is, it approached the House subpoenas not as a danger to privacy *per se*, but a danger to the office of the presidency.[392] For example, *Mazars* suggested that Congress's "open season" on third-party data presented concerns because "Congress could 'exert an imperious controul' over the Executive Branch and aggrandize itself at the President's expense."[393] In response, the Court imposed a new balancing test—not one based on privacy considerations, but rather one that reflects the "weighty concerns regarding the separation of powers" when congressional surveillance targets the President.[394]

Yet in doing so, it rendered a decision that is both over- and underinclusive as to privacy. *Mazars* is *underinclusive* because it protects only the President's information without offering any special

390. *Supra* notes 13–23 and accompanying text.
391. Trump v. Mazars USA, LLP, 140 S. Ct. 2019, 2034–35 (2020).
392. *Id.*
393. *Id.* at 2034 (quoting THE FEDERALIST NO. 71, at 484 (Alexander Hamilton)).
394. *Id.* at 2035.

considerations related to individual privacy.[395] The Court's opinion clearly acknowledges the expansive terrain in which Congress can use surveillance subpoenas, referring to it as an "open season" on third-party data.[396] But the balancing test it imposes is rooted solely in the President's unique position as "the only person who alone composes a branch of government."[397] As a result, *Mazars* does nothing for other public servants in whose information Congress may be interested, and nothing for individuals outside of the executive branch. Yet, in many cases, those are the individuals who find themselves in Congress's crosshairs. Indeed, by increasing the threshold for presidential information, *Mazars* may make it more likely that Congress will instead target those who lack the cloak of presidential power.

At the same time, *Mazars* is *overinclusive* because it limits the benefits of congressional surveillance. While *Mazars* dwells on the threat posed to traditional dynamics of intra-branch disputes by congressional surveillance, as I have argued, that shift is a feature, not a bug. *Mazars* portrays the House subpoenas as a deviation from a norm but overlooks the use of congressional surveillance as constitutional politics. As a result, *Mazars* limits the benefits of congressional surveillance without addressing its broader privacy costs, or even pausing to assess the varying degrees of information—from things like the content of private communications and files, location information and other revealing metadata, to basic business records—that congressional surveillance can potentially cover.[398] Instead, *Mazars* lumps it all together.

---

395. In effect, *Mazars* treats presidential "privacy" as an interest of the office, not the President as an individual. This would seem to present less of a challenge when information will not expose confidential matters involving the President's official duties, but even that may not be so simple. *See* Renan, *supra* note 37, at 1189–90 ("The privilege exists to sustain an ongoing institution. But the presidency cannot be fully disentangled from the persons of the [P]resident.").

396. *Mazars*, 140 S. Ct. at 2035.

397. *Id.* at 2034.

398. In contrast to *Mazars*, in a pure privacy approach, presidential information may be *less* protected than other information. For example, the presidency is a highly regulated job, and participation in a highly regulated industry significantly diminishes expectations of privacy. To be sure, in terms of Fourth Amendment requirements the "closely regulated industry . . . is the exception," City of Los Angeles v. Patel, 576 U.S. 409, 424 (2015) (quoting Marshall v. Barlow's, Inc., 467 U.S. 307, 313 (1978)), but it also represents a judgment that privacy interests may be so substantially diminished that judicial scrutiny may be relaxed. Indeed, Presidents might even "assume the risk" that Congress may choose to investigate their conduct, inside or outside of the Oval

This may be for the best, because it leaves room to explore alternative mechanisms to address the privacy implications of congressional surveillance without judicial intervention. Congress, as Part II argued, is a largely self-regulated body.[399] It does not need a court's opinion or legislative enactment to create an operative legal framework that binds member or committee behavior. Rather, Congress can establish rules to accommodate privacy considerations without ceding authority to judicial oversight or executive enforcement. It can do this at the chamber level or direct a committee to establish these rules.[400]

There are, to be sure, different ways to tackle this issue. But the obvious solutions, such as borrowing from the law enforcement context, risk repeating the *Mazars* mistake of elevating one perspective over the other. For example, like in the "super warrant" standard for wiretaps,[401] Congress could limit the use of its surveillance authorities to circumstances where alternative means to obtain the information are not available. It could also create use limitations on the data it collects. Or it could establish disclosure limitations on the data it collects. These limits would, in effect, require Congress to utilize first-person subpoenas for information, as opposed to first resorting to its surveillance powers. Use and disclosure limitations would prevent Congress from sharing large amounts of user information among congressional committees or retaining that data beyond its relevant time. Alternatively, these limits would impose transaction costs on Congress's decision to disclose private data.

Yet each of these limits reflects a background normative judgment that this Article has sought to rebut: that congressional surveillance is like other forms of government surveillance and should be similarly constrained. Instead, questions of design, not just the "what," but also

---

Office. From this perspective, heightened protections need not be extended to presidential information for privacy reasons.

399. *Supra* Part II.

400. This possibility is implied by chamber rules, such as Senate Rule 26.5(b), which lists exceptions to the default of holding open committee hearings when, for instance, it "will tend to charge an individual with crime or misconduct, to disgrace or injure the professional standing of an individual, or otherwise to expose an individual to public contempt or obloquy, or will represent a clearly unwarranted invasion of the privacy of an individual." S. DOC. NO. 110-1, at 43–44 (2008).

401. Jennifer S. Granick et al., *Mission Creep and Wiretap Act 'Super Warrants': A Cautionary Tale*, 52 LOY. L.A. L. REV. 431, 433 (2019) (explaining that a "super warrant" is required to permit government wiretapping under the Wiretap Act of 1968).

the "who," should begin with the recognition that congressional surveillance is a convergence of two distinct systems, one that operates within strict legal constraints and another that operates within fluid political constraints. Understanding these hybrid characteristics, as this Article has argued, is the necessary precondition to the normative project.

CONCLUSION

Congressional surveillance challenges traditional thinking about government surveillance. Courts, providers, and even congressional committees themselves will have to grapple with these authorities and their limits, navigating the uncertainty surrounding congressional surveillance. The challenge will be that congressional surveillance is a bit of an anomaly, and that the constraints on Congress are political and procedural, rather than statutory and substantive.

This is, to be sure, a scary proposition for students of government surveillance. On their own, process limits are rarely a reliable check on surveillance powers. But at the same time, congressional surveillance serves Article I purposes unlike other goals of government surveillance. How we approach congressional surveillance should therefore be grounded in its particular features, protecting privacy while empowering Congress in its constitutional role.