A RESPONSE TO PROFESSOR REBECCA WEXLER'S "PRIVACY AS PRIVILEGE"

*Vikas K. Didwania**

Privacy law recently was rocked by a novel legal argument made in the Harvard Law Review by Professor Rebecca Wexler. According to the article, due to federal privilege law, criminal defendants must be allowed to subpoena user content from social media companies. The argument was novel because the text of the federal Stored Communications Act has long been read to preclude it. The potential privacy implications of this argument are substantial: a decision giving criminal defendants and every other litigant access to user communications would open up for frequent discovery the most intimate online communications, photographs, videos, and other content belonging to billions of users worldwide.

This Article argues that Professor Wexler's interpretation of the Stored Communications Act is wrong. Cases dating back to the telegram era of the late nineteenth century and continuing to modern day consistently show that Congress does not have to use any specific language to block defendants' access to information. Rather, courts have applied the plain text of the Stored Communications Act, which, alongside the Act's structure and purpose, shows that criminal defendants are banned from obtaining content. Moreover, this Article cautions that courts should not rely on Professor Wexler's new approach because doing so would both create a doctrinal mess in a carefully structured statute and strain courts with difficult policy decisions involving the privacy of billions of people.

This Article ends by describing the numerous tools already available to defendants for obtaining online content. It shows that in almost all circumstances, defendants will be able to obtain the specific evidence they seek, either from the government or through one of the exceptions provided in the Act.

* Lecturer in Law, University of Chicago Law School; Assistant United States Attorney, United States Attorney's Office, Northern District of Illinois. Affiliations are listed for identification purposes only. All statements of fact, opinion, or analysis expressed are mine and do not necessarily reflect the official positions or views of the Department of Justice, the U.S. Attorney's Office, or any other U.S. government agency. Nothing in the content of this Article should be construed as asserting or implying U.S. government authentication of information or agency endorsement of the author's views. For thoughtful comments to earlier drafts, the author thanks Stephanie Holmes Didwania, Orin Kerr, Matthew Tokson, and Rebecca Wexler.

Introduction

Since 1986, the federal Stored Communications Act (SCA) has protected the privacy of online communications.[1] It does so by prohibiting online companies like Facebook from disclosing user content except in certain limited circumstances listed in the law. Civil litigants and defendants in criminal cases have sometimes sought to compel online companies to give them access to this private user content. Because of the SCA's broad prohibition, courts have uniformly refused to force online companies to give criminal defendants and private litigants access to these private online communications.

1. Title II of the Electronic Communications Privacy Act, 99 P. L. 508, 100 Stat. 1848, codified at 18 U.S.C. §§ 2702–2712.

Recently, commentators and litigants have been creatively—yet thus far unsuccessfully—challenging this prohibition within the SCA.[2] Perhaps most notably, a recent article written by Professor Rebecca Wexler and published in the Harvard Law Review argues that the SCA must allow criminal defendants to compel (such as subpoena) user content from social media companies.[3]

The text of the SCA precludes this argument. The SCA states that online companies "shall not knowingly divulge to any person or entity the contents of a communication."[4] Throughout this Article, I refer to this provision as the SCA's *disclosure ban* (because it *bans* online companies from *disclosing* communications). This disclosure ban prohibits both voluntary disclosures by online companies and disclosures compelled by court orders, except in certain limited circumstances. For example, one of the exceptions allows criminal defendants to get access to online communications by obtaining the consent of the user.[5] Another exception allows criminal defendants to compel online companies to give them access to non-content user information—but not user content.[6] The disclosure ban also does not prevent criminal defendants from getting the user communications directly from the user. But criminal defendants have sought to directly compel online companies to disclose user content without user consent. The SCA does not contain an exception allowing criminal defendants to do that.

Wexler argues that courts have incorrectly interpreted the SCA's disclosure ban. Wexler's argument is one of statutory interpretation. According to Wexler, despite the disclosure ban, criminal defendants can force online companies to give them user content. The reason lies in a canon of construction referred to as the *presumption against privileges*. Wexler argues that a statute creates a legal *privilege* when it blocks parties from accessing otherwise relevant evidence, even with a court order. According to Wexler, reading the SCA's disclosure ban as

2. *See, e.g.*, Facebook v. Pepe, 241 A.3d 248 (D.C. Court of Appeals 2020); Facebook v. Wint, 199 A.3d 625 (D.C. Court of Appeals 2019); Facebook Inc. v. Superior Court, 417 P.3d 725 (Cal. 2018); United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015). There are also many other lower federal and state court cases, as well as petitions for certiorari in the Supreme Court, *e.g.*, Facebook, Inc. v. Superior Court, 140 S. Ct. 2761 (2020). As for articles, see, among others, Rebecca Wexler, *Privacy as Privilege: The Stored Communications Act and Internet Evidence*, 134 HARV. L. REV. 2721 (2021); Rebecca Steele, Note, *Equalizing Access to Evidence: Criminal Defendants and the Stored Communications Act*, 131 YALE L. J. 1385 (2022).

3. *See generally* Wexler, *supra* note 2.

4. 18 U.S.C. § 2702(a)(1).

5. 18 U.S.C. § 2702(b)(3).

6. 18 U.S.C. §§ 2702(a)(3), (c)(6).

prohibiting access for criminal defendants would mean the ban creates a legal privilege.

However, according to Wexler's presumption against privileges canon, a statute should be interpreted not to create a legal privilege unless the privilege is clearly stated in the statute. Wexler reads the SCA's disclosure ban to lack the required clear statement, because it does not contain specific language about privilege, discovery, or legal process. The disclosure ban does not explicitly say, for example, that disclosure is "immune from legal process." Wexler does not analyze the plain text of the SCA's disclosure ban first to determine whether it is ambiguous as to whether it bans disclosure pursuant to defense subpoenas. Instead, Wexler applies the presumption to conclude that the disclosure ban is ambiguous because it does not contain a "clear statement" such as "immune from legal process." The supposed lack of this clear statement means courts should interpret the SCA to allow disclosure to defendants through legal process. Otherwise, the disclosure ban would create a legal privilege without the required clear statement.[7]

This Article explains why this argument is incorrect. First, because the text of the SCA is unambiguous, a canon of construction—such as the presumption against privileges—should not be used to interpret it. Second, allowing defendants to subpoena service providers under the SCA would be inconsistent with the text of the SCA and would create a statutory mess. That is further evidence that the presumption should not be applied. Lastly, this Article demonstrates that cases from the era of telegrams reached similar conclusions. During this era, states enacted laws similar to the SCA—banning the disclosure of telegram communications—and courts applied the text of these statutes rather than the presumption against privileges.

The stakes of the debate are high: the privacy of the communications of billions of people. For example, in December 2020, 2.6 billion people were active daily on at least one Facebook product (Facebook, Facebook Messenger, WhatsApp, Instagram).[8] That means about one-third of the world's entire population was active on a Facebook product every day. These users share seventeen billion photos just on

7. See Wexler, *supra* note 2, at 2725. The following case and articles also have supported this novel argument: Colone v. GitHub, No. 20-1474, 2021 WL 3552182 (Aug. 6, 2021); § 5437 Exceptions—Act of Congress, 23A FED. PRAC. & PROC. EVID. § 5437 (1st ed.); Kiel Brennan-Marquez, *Beware of Giant Tech Companies Bearing Jurisprudential Gifts*, 134 HARV. L. REV. FORUM 434 (2021).

8. Annual Report 2020 (SEC Form 10-K), FACEBOOK 52 (2020), https://s21.q4cdn.com/399680738/files/doc_financials/2020/ar/2020-Annual-Report.pdf.

Facebook Messenger every month.[9] Undoing the ban in the manner proposed by Wexler and others could open up a wide swath of electronic communications to additional production in almost every civil or criminal case in federal, state, and local litigation and in administrative proceedings.

Part I walks readers through the statutory text. The text of the SCA disclosure ban broadly and unambiguously prohibits service providers from disclosing content; it states that service providers "shall not knowingly divulge to any person or entity the content of a communication." The statute's text plainly prohibits service providers from disclosing content in any circumstance—either voluntarily or pursuant to compelled process like a subpoena—to individuals, including criminal defendants. Because the text is clear, there is no need to apply a canon of construction like the presumption against privilege. Nonetheless, Part I also tackles the presumption against privilege canon. The problem with Wexler's interpretation, as explained beginning in Part I.B, is that it is inconsistent with the statutory text and structure of the SCA.

Part II considers three cases in which the Supreme Court interpreted disclosure bans in other contexts, which Wexler refers to as the Supreme Court "trilogy." Part II explains that when read properly, the trilogy cases are entirely consistent with the textual analysis contained in Part I and inconsistent with Wexler's novel argument. There is no requirement that a privilege be explicitly written into the statute.

Part III examines older cases decided by state and lower federal courts dealing with disclosure bans for telegrams. These courts also rejected arguments about privilege and instead looked to the text of the statute to understand the scope of the disclosure ban.

Finally, Part IV demonstrates why the current regime is not as harsh for defendants as Wexler has suggested. It shows that in almost all circumstances, defendants *will* be able to obtain the evidence they need: either from the government or by using one of the exceptions already provided in the SCA. It also explains why the disclosure expansion desired by Wexler must be done by Congress, not the courts. Privileges reflect difficult, sensitive policy judgments. On one hand, the search for truth is unquestionably critical and privileges inhibit this search. On the other hand, privileges protect and encourage critical societal interests, like the privacy of intimate communications of bil-

9. Andrew Hutchinson, *Facebook Messenger By the Numbers 2019*, SOCIAL MEDIA TODAY (May 1, 2019), https://www.socialmediatoday.com/news/facebook-messenger-by-the-numbers-2019-infographic/553809/.

lions of users. Congress must create a comprehensive disclosure scheme to balance the complex and important interests at stake and determine the extent of court oversight.

I.
STATUTORY INTERPRETATION OF THE DISCLOSURE BAN

Wexler argues that courts have improperly read the SCA's disclosure ban to prohibit defense subpoenas for user content.[10] According to Wexler, reading the disclosure ban to prohibit defense subpoenas creates an evidentiary privilege.[11] That is because shielding relevant information from legal process is an evidentiary privilege, like the attorney-client privilege or the privilege against self-incrimination.[12] The question of what constitutes an evidentiary privilege is a complicated one. This Article presumes that by blocking defense subpoenas, the disclosure ban in the SCA creates an evidentiary privilege. But as Wexler recognizes, it is permissible for statutes to create evidentiary privileges.[13] The question is whether Congress intended to create such a privilege in a particular statute. Wexler's novel argument fundamentally presents a question of statutory interpretation: does the text of the SCA ban the disclosure of content through defense subpoenas?[14]

Wexler argues that a particular principle of statutory construction, namely the presumption against privileges, requires interpreting the disclosure ban to allow defense subpoenas for user content.[15] This presumption prevents "courts from construing a federal statute to block legal process unless the plain text of the statute clearly indicates congressional intent to create a privilege."[16] According to Wexler, Congress must use specific phrases such as "immune from legal process" or "shall not be subject to discovery" to block legal process and create an evidentiary privilege.[17] Wexler applies this canon of construction—the presumption against privileges that requires a clear statement—to conclude the SCA's disclosure ban is ambiguous. The SCA's disclosure ban does not contain the required clear statement, so pursuant to the presumption, it must be ambiguous. Since courts

10. Wexler, *supra* note 2, at 2725.
11. *Id.*
12. *Id.* at 2746-47.
13. *Id.*
14. Legal process refers to process issued under a court's authority compelling the production of documents or testimony, such as subpoenas and search warrants.
15. Wexler, *supra* note 2, at 2757.
16. *Id.*
17. *Id.* at 2763–64.

sometimes apply a canon of construction to resolve ambiguity, Wexler once again applies the presumption against privileges to conclude that the ambiguity should be resolved in favor of disclosure and against creating a privilege.

As discussed below, Supreme Court cases have found disclosure bans to block legal process even without the clear statement. As a result, Wexler alternatively argues that statutes can create "implied privileges" and block legal process without the clear statement. But, according to Wexler, these implied privileges exist only in certain "narrow" circumstances, such as when the statute contains a broad nondisclosure mandate with minimal or no exceptions.[18] According to Wexler, because the SCA can be read in a way not to block defense subpoenas (because it does not use the specific phrases she identifies), it should be read this way.[19]

As explained below, section 2702(a) of the SCA contains a broad disclosure ban and the text unambiguously prohibits social media companies from disclosing user content to anyone, including through compelled disclosures such as subpoenas. Section 2702(b), in turn, contains exceptions to 2702(a)'s broad disclosure ban, including a specific exception for disclosure of content pursuant to *governmental* subpoenas and search warrants. The statute contains no exception for disclosure of content pursuant to non-governmental subpoenas. Canons of construction, such as the presumption against privilege, are used to resolve ambiguity, not to dictate how Congress should word statutes. Here, presumptions or other canons of construction cannot be used because there is no ambiguity to resolve. The only plausible reading of the disclosure ban is that it blocks defense subpoenas, and courts correctly have read it do so. Subsequent parts of this Article explain how Wexler also appears to have misread what the presumption against privileges canon requires.

A. The Disclosure Ban's Plain Meaning

Section 2702(a)(1) of the SCA bans the disclosure of content:

> Except as provided in subsection (b) or (c), a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.[20]

18. *Id.* at 2771–73.

19. *Id.* at 2773–74.

20. 18 U.S.C. § 2702(a)(1). There is an almost identical provision for remote computing services. Subsection (c) concerns disclosure of non-content information and therefore is not discussed in detail.

The plain language of § 2702(a)(1) makes clear that Congress sought to ban any disclosure of content by service providers, whether compelled or not, to any person or entity unless the disclosure falls under an exception contained in 2702(b) or 2702(c).[21] Individuals, including criminal defendants, are "any persons"[22] and they therefore fall within the scope of those who cannot receive content by service providers (and, as discussed next, no listed exception applies to them).

Sections 2702(b) and (c) of the SCA contain exceptions to the broad disclosure ban laid out in § 2702(a). Like the disclosure ban itself, the exceptions to the disclosure ban are unambiguous. None of the exceptions allows for content disclosures pursuant to defense subpoenas. Instead, they narrowly focus on disclosures authorized by the sender or receiver, the needs of service providers to operate their business, and public safety.[23] Eight of the nine exceptions are for circumstances wholly unrelated to compelled disclosures. They include disclosures to employees and others necessary for the service's operation; disclosure of the communication to its intended recipient; disclosures pursuant to the consent of the sender or recipient; emergency disclosures to the government in situations involving death or serious physical injury; and disclosures to the National Center for Missing and Exploited Children, among others.[24]

The inclusion of these basic, necessary exceptions illustrates the ban's breadth. The fact that Congress perceived the need to include exceptions necessary to the most basic functioning of the service provider, such as disclosing the communication to the recipient or to an employee, shows the ban really does cover every imaginable kind of disclosure. Also, as discussed more in Part IV, some of these exceptions can and have been used by criminal defendants to obtain content. For example, content can be disclosed to the sender or recipient, so the defense can obtain it from these parties.

The remaining exception allows disclosures pursuant to section 2703.[25] Section 2703, titled, "Required disclosure of customer com-

21. *See, e.g.*, Lawson v. FMR LLC, 571 U.S. 429, 440 (2014) ("In determining the meaning of a statutory provision, we look first to its language, giving the words used their ordinary meaning.") (internal quotation marks omitted).

22. The Supreme Court repeatedly has noted that the term "any person" has a "naturally broad and inclusive meaning." *See, e.g.*, Pfizer v. Gov't of India, 434 U.S. 308, 312 (1978).

23. *See* S. REP. 99-541, at 37–38 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3591 ("The exceptions to the general rule of nondisclosure provided in subsection (b) fall into three categories.").

24. 18 U.S.C. § 2702(b).

25. The third exception also refers to 18 U.S.C. §§ 2511(2)(a) and 2517, both of which concern disclosures of communications intercepted pursuant to the Wiretap Act

munications or records," comprehensively regulates how a service provider can be legally compelled to disclose information, but only to the government. Subsection (a) allows a "governmental entity" to obtain content from an electronic communication service provider through a search warrant.[26] Similarly, subsection (b) allows a "governmental entity" to obtain content from a remote computing service through a search warrant.[27]

If Congress had wanted to include an exception for defense subpoenas or for all compelled disclosures generally, it would have said so in the statute.[28] It did not. Moreover, as discussed below, Congress included an exception for defense subpoenas in another part of the SCA and has done so in other statutes, so it knows how to do so. But there is a broader point here as well: the explicit exception of certain kinds of legal process reveals that disclosures pursuant to compulsory process (like subpoenas) are within the scope of the disclosure ban.[29] If compulsory process were outside the scope of the ban, Congress would not have needed to create additional exceptions for certain types of compulsory process.

A defendant plainly is not authorized to compel disclosure of content under sections 2702 and 2703.[30] Every court to have considered this question of statutory interpretation has come to the same con-

---

and not stored communications. These sections also do not mention any compelled disclosures to defendants in criminal cases.

26. Although the statutory text allows the government to obtain certain content with less than a search warrant, as a practical matter, most service providers now demand a warrant, and most prosecutors seek a warrant, for the content of communications regardless of its age, whether it is opened or unopened, or how it is stored. *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/help/494561080557017 (last visited May 22, 2023) (noting a search warrant is required for any stored content).

27. Although the statutory text allows the government to obtain certain content with less than a search warrant, as with subsection (a), prosecutors use a warrant to obtain content regardless of notice to the subscriber.

28. *See* Cyan v. Beaver Cnty, 138 S. Ct. 1061, 1070 (2018) ("But if Congress had intended to refer to the definition in § 77p(f)(2) alone, it presumably would have done so—just by adding a letter, a number, and a few parentheticals.").

29. *See* Brown v. Maryland, 25 U.S. (12 Wheat.) 419, 438 (1827) ("[T]he exception of a particular thing from general words, proves that, in the opinion of the lawgiver, the thing excepted would be within the general clause had the exception not been made").

30. A defendant is not a "governmental entity," which is defined as "a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711(4). Nor could a court issuing the subpoena be considered a "governmental entity" because (a) the statute separately uses the word "court" to refer to courts; and (b) a governmental entity "obtains" process, "offers specific and articulable facts," "requests" the preservation of evidence before going to court, and so on, all of which can only refer to investigative agencies, not courts. *See* 18 U.S.C. § 2703.

clusion.[31] The text of the SCA leaves little discretion to the service provider, the parties, or courts in implementing the disclosure ban. It uses the word "shall" in banning disclosures[32] and creates a narrow set of exceptions that also leave little discretion in implementation. Congress used the word "shall" to make clear the ban was a command that left nothing to discretion.[33] Courts, for example, are not allowed to balance a party's need for the information with the costs to privacy. Congress already accounted for this balance in enacting the comprehensive scheme found in the SCA.

The use of "shall" also ensures that the content of communications is protected in a predictable manner. The report prepared by the Senate Judiciary Committee recommending passage of the SCA explains that a purpose of this tight ban was to reduce "legal uncertainty," which "discourage[s] potential customers from using innovative communications systems" and may "discourage American businesses from developing new innovative forms of telecommunications and computer technology."[34] As discussed in more detail below, interpreting the SCA to allow subpoenas for content would create many uncertainties about how to implement disclosures in a variety of civil, criminal, and administrative proceedings, thereby defeating one of the central purposes of the ban—certainty.

It is also worth noting that interpreting the disclosure ban to prohibit subpoenas other than those specifically excepted is also consistent with the purpose of the statute. Congress enacted the SCA to expansively protect privacy.[35] The legislative history confirms that Congress was concerned with protecting privacy in its many forms—

---

31. *See* Wexler, *supra* note 2, at 2725 (criticizing the "consensus view" among courts to disallow defense subpoenas); *Id.* at 2722 (noting "[e]very appellate court to rule on this issue" has come to the same conclusion).

32. Other statutes use the more discretionary "may disclose" terminology. *See, e.g*., 26 U.S.C. § 6103 (Secretary of Treasury "may disclose" taxpayer information in various circumstances); 18 U.S.C. § 2517(1) (law enforcement "may disclose" contents of intercepted communications in certain circumstances).

33. Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26, 35 (1998) (observing that "'shall'" typically "creates an obligation impervious to . . . discretion").

34. S. REP. 99-541, at 5.

35. *Id.* at 3 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information . . . . It 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."); *see also* Microsoft Corp. v. United States, 829 F.3d 197, 217 (2d Cir. 2016) ("Having done so, we conclude that the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications.").

not just from government surveillance but also by prohibiting disclosure to private parties.[36] At the time the SCA was enacted, Congress recognized it was creating a broad disclosure ban that would reach all kinds of disclosures. For example, the Senate Judiciary Committee report confirms the ban's breadth, describing that "section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee of intended recipient," and "[s]ubsection (b) of this new section provides exceptions to the general rule of nondisclosure provided in subsection (a)."[37] These statements evince a congressional purpose to "generally" prohibit disclosures to "any person." Any effort to undermine these protections faces a high hurdle in light of the broad statutory language and purpose.

B. Consequences of Allowing Compulsory Process

The preceding section showed that one cannot read the SCA's disclosure ban to exclude compelled disclosures like subpoenas from the ban—unless those subpoenas are explicitly allowed by the statute. This section explains why such a reading of the SCA would also create results plainly inconsistent with the text, structure, and goals of the statute, which is further evidence that Congress did not exempt defense subpoenas from the disclosure ban.

1. Inconsistent with the statutory structure

Allowing compelled disclosures to avoid the SCA's disclosure ban is contrary to the statutory structure of the SCA.[38] Much of the discussion so far has been about "content" information but the SCA's treatment of non-content information is also illustrative. Non-content information is considered less private than the content of communications.[39] Non-content information includes, for example, the name, ad-

36. S. REP. 99-541, at 3 ("Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others are readily available in the American market today.")

37. S. Rep. No. 99-541, at 37.

38. *See* Lockhart v. United States, 577 U.S. 347, 349–52, 356 (2016) (explaining that reliance on a canon "can assuredly be overcome by other indicia of meaning," and that such issues are "fundamentally contextual questions").

39. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009).

dress, and phone number of the subscriber.[40] Congress explicitly allowed non-governmental entities, such as criminal defendants, to obtain non-content information, whether voluntarily or through subpoenas.[41] 2702(c) explicitly allows disclosure of non-content information to non-governmental entities, such as defendants.

For the more private "content" information, Congress allowed limited disclosure to a narrow group consisting of only governmental entities and required the government to use the most onerous legal process: a search warrant. User content, because it is so private, cannot be disclosed except in a criminal investigation where the government has shown to a magistrate judge that there is probable cause to believe the content contains evidence of a crime or the account was used as an instrumentality of a crime. However, Congress allowed non-governmental entities to obtain the less private non-content information without much difficulty. The distinctions Congress drew were both explicit and rational (at least in 1986). Given the detailed scheme Congress set up and the distinctions it created, it is difficult to conclude that somewhere in the statute Congress left hidden an exception for non-governmental content subpoenas.

2. Inconsistent with the statutory outcomes

Allowing all compelled disclosures, or even just defense subpoenas for content, would create a statutory mess. This result is further evidence that the statute is not amenable to the interpretation Wexler advocates, namely that the disclosure ban allows for defense subpoenas.

Congress sought to strictly protect content and required a search warrant for its disclosures. Criminal defendants cannot obtain search warrants.[42] What process, then, would a court require for the defense to access third-party content? Search warrants are unavailable to the defense. And there does not appear to be a textual basis for defense subpoenas to be issued under the SCA. Section 2703, which governs compelled disclosures, is explicitly limited to process issued on the government's behalf. What would be the legal standards for defendants to obtain such process? Would it be the same standard as for defendants to obtain non-content information? That approach would be inconsistent with the statutory scheme which is more protective of content information. These issues are not necessarily difficult for a

40. *Id.* at 2112, 2128–29.

41. 18 U.S.C. §§ 2702(a)(3), (c)(6).

42. *See* FED. R. CRIM. P. 41 (limiting search warrants to requests of federal law enforcement and government attorneys).

policymaker to resolve. But they are impossible for a court trying to interpret a statute that is entirely silent on the topic. In allowing defense subpoenas for content, courts would have to invent statutory requirements out of whole cloth—with no guidance and no authority to do so.

Consider next the argument that courts should ignore section 2703—the section that expressly governs compelled disclosures—and conclude that defense subpoenas could be governed by Federal Rule of Criminal Procedure 17 instead. Rule 17 governs the issuance of subpoenas in criminal cases. Courts could simply apply Rule 17. But this approach runs headlong into the text and structure of the SCA.

The SCA allows the defense to obtain non-content information through a Rule 17 subpoena. It would be inconsistent with the statute's structure to allow the defense to obtain content information through an identical process with identical standards. Again, the SCA is clear that it sought to protect content more stringently and require higher standards for its disclosure.[43]

Allowing the defense to obtain content through a Rule 17 subpoena, without more explicit instruction from Congress, would create other oddities. It would create a much more difficult standard for the government to obtain content (a search warrant), whereas the defense could simply use a Rule 17 subpoena. The standard for a Rule 17 subpoena is that the subpoena must not be unreasonable or oppressive.[44] This standard is substantially lower than what is required for a search warrant because it does not require "probable cause." Rule 17, though, treats the government and the defense equally as to the process for issuing subpoenas, the standards for issuing subpoenas, the fees for subpoenas, and so on. Yet, Wexler's approach would create different standards for the government and the defense in obtaining

43. Section 2703 set up a detailed, "pyramidal structure" for disclosure. *See Microsoft Corp.*, 829 F.3d at 207. Disclosure of less sensitive information, such as subscriber records, requires only a subpoena. *See* 18 U.S.C. § 2703(c)(2). More sensitive information requires a court order with a specific standard the government must meet: "specific and articulable facts" that the information "are relevant and material to an ongoing criminal investigation." *See* 18 U.S.C. §§ 2703(c)(1)(B), (d). And the most sensitive information—content—requires a search warrant. *See* 18 U.S.C. §§ 2703(a), (b).

44. *See* FED. R. CRIM. P. 17(c); *see also* United States v. Nixon, 418 U.S. 683, 698 (1974) ("A subpoena for documents may be quashed if their production would be 'unreasonable or oppressive,' but not otherwise."); United States v. Smith, No. 19-CR-00669, 2020 WL 4934990, at *2–4 (N.D. Ill. Aug. 23, 2020) (detailing how courts disagree about exactly how to define "unreasonableness" in the context of third-party subpoenas by defendants).

content. Congress of course could authorize this difference, but a court cannot without a textual basis.

Allowing the production of user content through simple subpoenas would severely undermine the privacy protection of the SCA. Congress required search warrants to obtain content because of how sensitive and private user content is. Search warrants are only available to the government. As discussed in more detail in Part IV, allowing disclosures through subpoenas creates significant privacy issues. Often, subpoenas are issued without any court oversight and the standard for a subpoena can be much lower than that for a search warrant. The lack of court oversight may also leave open the possibility of re-disclosure of private content by defendants or their attorneys. And the privacy implications can be massive because service providers will produce the entire account instead of just the relevant information, which can mean gigabytes of data involving communications with hundreds or thousands of subscribers.[45]

Another inconsistency of Wexler's approach would be with section 2706 of the SCA, which generally requires payment to the service provider for the burdens of complying with the government's compulsory process. The traditional default rule is that witnesses are not compensated for complying with legal process because such compliance is seen as a societal obligation.[46] With the SCA, Congress flipped this traditional rule to require payment to online companies for compliance with government subpoenas. In this way, Congress furthered the purpose, as described above, of encouraging innovation by not burdening startups and other innovators with the costs of complying with onerous legal processes. Meanwhile, Rule 17 maintains the traditional rule.[47] Rule 17 defense subpoenas for content would be inconsistent with the SCA's reimbursement scheme and undermine the broader statutory purpose of encouraging innovation. It would also create another disparity between the government and the defense: the government would pay greater costs to obtain the same evidence. Again, Congress certainly could decide that the government must pay but defendants must not in criminal cases. But this outcome is without legal basis as a matter of judge-imposed policy.

45. *See, e.g.*, United States v. Aboshady, 951 F.3d 1, 5 (1st Cir. 2020) (describing the wide extent of a search warrant for the documents within a defendant's Google account, which for Aboshady involved over 430,000 documents); United States v. Purcell, 967 F.3d 159, 173–75 (2d Cir. 2020).

46. *See* Hurtado v. United States, 410 U.S. 578, 588–89 (1973).

47. *See id.*

Wexler's approach also would create an inconsistency with section 2707 of the SCA, which created remedies for violations of the SCA. Subsection (g) makes it unlawful for the government to willfully disclose information it obtained through compulsory process. Subsection (d) sets up an administrative disciplinary process for re-disclosure violations. There are no similar provisions for defendants who obtained information through compulsory process because Congress did not plan for defense disclosures of content. Unilaterally allowing defense subpoenas for content would undermine Congress's careful and comprehensive scheme to protect electronic content and remedy SCA violations.

Consider also section 2703(e) of the SCA, which immunizes service providers from any "cause of action . . . in any court . . . for providing information, facilities, or assistance" in accordance with compulsory process issued "under this chapter." The only compulsory process issued "under this chapter" of the SCA is governmental process issued under section 2703. As a result, any defense subpoena would not be issued "under this chapter." Section 2703 makes no allowance for the issuance of defense subpoenas for content. Even if the disclosure ban is read not to block defense subpoenas, such subpoenas could not be issued under the SCA. Due to the immunity provision of section 2703(e), a service provider cannot be sued for complying with any governmental compulsory process under 2703. Yet, the service provider could be sued for disclosing content pursuant to Rule 17 defense subpoenas, which are not subpoenas issued under the SCA. This inconsistent treatment does not make sense. More than that, it undermines the entire purpose of the immunity provision by destroying certainty, especially for small startups, and undermines Congress's efforts to support nascent industries. It exposes these startups (as well as large companies) to litigation in a rapidly developing area, both technologically and legally. And it creates a wide chasm between the government's efforts to obtain process and the defendant's, without any textual basis. There is no fair way to read the SCA as allowing such an outcome—and certainly not based on hidden, implied exceptions.

The SCA appears to be unambiguous in banning compelled disclosure of content except through governmental search warrants.

C. The Difference Between Breadth and Ambiguity

Unpersuaded readers may note the disclosure ban itself says nothing *explicit* about compulsory process or even defense subpoenas for content. The claim may be that this lack of specificity means the

statute is ambiguous as to whether it allows defense subpoenas. To resolve this ambiguity, courts could turn to canons of construction, as they traditionally do. Here, the argument goes, the applicable canon is the presumption against privilege, and it would require construing the supposedly ambiguous disclosure ban to allow all compelled disclosures. The flaw with this line of argument is that lack of specificity is not the same as ambiguity. Sometimes, as here, the lack of specificity is instead a signal of breadth. To understand why, it is necessary to see how the disclosure ban works in connection with the exceptions Congress created. In essence, because Congress was seeking to create a broad ban, it explicitly listed the limited instances in which disclosure was allowed—rather than list all the many instances in which disclosure was prohibited.

As described above, the general ban creates a default that prohibits disclosures in *all* circumstances, whether voluntary or compelled. It is worded broadly. The list of exceptions allows certain disclosures that would otherwise be prohibited by the broad ban. The "except" clause contained within the broad ban indicates that in certain circumstances, when there is a conflict, the exception should govern. As the Supreme Court has explained, "Thousands of statutory provisions use the phrase 'except as provided in. . .' followed by a cross-reference in order to indicate that one rule should prevail over another in any circumstance in which the two conflict . . . ."[48] If a circumstance (like defense subpoenas) is not on the specified list of exceptions, there is no conflict or ambiguity; a court must abide by the default provision banning all disclosures.

Consistent with the natural way to read such provisions, the Supreme Court has read "except" clauses as providing the sole exceptions to a general provision.[49] In one case, it stated, "[w]here Congress explicitly enumerates certain exceptions to a general prohibition, additional exceptions are not to be implied, in the absence of evidence of a contrary legislative intent."[50] The same is true with the SCA: Congress specified the exemptions from the broad ban on disclosure, and

48. *See Cyan*, 138 S. Ct. at 1070.

49. *See, e.g.*, United States v. Resler, 313 U.S. 57, 59 (1941) ("The phrase 'Except as provided in section 213 (313)' [in section 212(b)] was intended to remove from the sweep of § 212(b) only those transfers which were within the compass of § 213."); Coeur Alaska, Inc. v. Se. Alaska Conservation Council, 557 U.S. 261, 273 (2009) (reading the clause "Except as provided in . . . [CWA § 404, 33 U.S.C. § 1344], the [EPA] Administrator may . . . issue a permit for the discharge of any pollutant" as allowing the EPA to issue "permits for the discharge of any pollutant" with "one important exception").

50. TRW Inc. v. Andrews, 534 U.S. 19, 28 (2001) (quotations omitted).

only Congress can add additional ones, such as for defense subpoenas. Wexler's approach instead would have courts add in an exception for defense subpoenas.

Consider the converse. To find ambiguity in the broad ban would mean Congress has to list the specific instances where the ban applies: that it applies to voluntary and compelled disclosures; to verbal, paper, and electronic disclosures; to disclosures of old and new content; and so on. Yet, as a matter of statutory interpretation, the rule is that Congress's "broad, sweeping language should be given broad, sweeping application."[51] An alternative approach would be unworkable; it would require Congress to imagine into the future all possibilities and list them. Restricting the ban from applying to unmentioned scenarios fails to give effect to the entire statutory scheme. Scenarios covered by the ban are not mentioned precisely because the ban is broad and covers a wide range of scenarios.

In other instances where Congress sought to exempt all compelled disclosures from a disclosure ban, as Wexler suggests is the case with the SCA, Congress created a specific exemption broadly allowing disclosures pursuant to legal process.[52] This approach shows that Congress knows how to exempt all compelled disclosures from disclosure bans when it wants to. Congress did not create a similar broadly worded exception in the SCA.

One might ask: what if Congress did not intend to ban defense subpoenas and simply did not anticipate that the broad ban would block defense subpoenas? Yet, as mentioned above, Congress did address non-governmental disclosures in other circumstances, which is strong evidence that Congress intended to create the scheme it actually created. Congress recognized that it was acting in a world with rapidly changing technology, but at the same time, it wanted to bring certainty to the legal landscape. The only way to accomplish that is by enacting a broad provision that can reach a broad set of anticipated and unanticipated situations. As the Supreme Court has explained, "the fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth."[53] The ban's breadth is the intended feature of the SCA, and it is how Congress locked in broad protections for private communications.

---

51. *See* Consumer Elecs. Ass'n v. FCC, 347 F.3d 291, 298 (D.C. Cir. 2003) (citing New York v. Fed. Energy Regulatory Comm'n, 535 U.S. 1, 21 (2002) and PGA Tour, Inc. v. Martin, 532 U.S. 661, 689 (2001)).

52. *See, e.g.*, 15 U.S.C. § 330b(c)(2); 47 U.S.C. § 605(a).

53. *Martin*, 532 U.S. at 689 (quotations omitted).

The case *TRW v. Andrews*[54] shows how presumptions cannot be used to create additional exceptions to an otherwise broad provision. The Fair Credit Reporting Act requires actions to be brought within two years of when the liability arises except where the defendant had willfully misrepresented certain material information.[55] In the latter circumstance, the action could be brought within two years of the plaintiff's discovery of the misrepresentation. The court of appeals in *TRW* applied a presumption in favor of the discovery rule to imply an exception allowing actions to be brought within two years after the plaintiff knows or has reason to know they were injured, even when the misrepresentation exception did not apply.[56] Like Wexler's argument, the court of appeals held that Congress must "expressly" legislate otherwise to overcome the presumption.[57]

The Supreme Court reversed. The Court noted that it had never endorsed the view that Congress must expressly reject a discovery rule (which, as explained below, is also true about the presumption against privilege).[58] The Court next explained that because Congress had explicitly enumerated certain exceptions, courts could not imply others.[59] In fact, the explicit enumeration of a more limited discovery rule implied that Congress had rejected the broader discovery rule.[60] All of this reasoning applies to the SCA's disclosure ban. The background presumption against privilege does not allow courts to imply additional exceptions to the ban. Importantly, Congress specifically exempted a narrower class of legal process, which implies that it rejected a broader exemption for all legal process. Alternatively, to see how presumptions like the presumption against privilege works in the context of a statute that is ambiguous, see the discussion in Part III below of the case *Pierce County v. Guillen*.

One might wonder: why didn't Congress use specific language like "immune from legal process" in the SCA's disclosure ban to make clear that the discovery ban covers legal process? It has done so in other statutes. Is Congress's decision to omit this language evidence that it sought to allow legal process under the SCA? The answer is no, because this specific language only makes sense in certain circumstances that are not applicable under the SCA. A provision like "immune from legal process" can be too broad for some situations

54. *Andrews,* 534 U.S. at 19.
55. *Id.* at 22.
56. *Id.* at 26.
57. *Id.*
58. *Id.* at 27–28.
59. *Id.* at 28.
60. *Id.*

involving statutory privileges. The provision and others like it do not work if Congress wants to allow certain legal process, such as search warrants, but not others, like subpoenas. Along the same lines, this language does not work if Congress wants to allow certain entities (like the government) to be able to use legal process but not so for other entities (like private parties). The SCA did not seek to bar all compulsory process for content. It allowed a narrow set of compulsory processes issued by governmental entities to service providers. It is therefore unlikely the statute would contain the broad compulsory process language that Wexler would require.

On the other hand, including language like "immune from legal process" can be too *narrow* if Congress wants to ban all kinds of disclosure, not just those compelled by legal process. In the SCA, Congress wanted to broadly ban voluntary and compelled disclosures by service providers, so it would have made little sense to use a provision only about legal process instead of the broader provision it did use. In the Census Act, for example, Congress wanted *not* to ban voluntary disclosures by businesses of their retained reports—it did not care what businesses chose to do with their own information. Another example is tax returns: taxpayers can do what they wish with their tax returns but the same is not true for tax returns held by the Internal Revenue Service. These statutes therefore could have more limited disclosure bans focused on making disclosure "immune from legal process."

The lack of a specific provision like "immune from legal process" in the SCA is not a "powerful sign" against statutory privileges.[61] Instead, in the context of statutory interpretation, it can be a sign of the ban's breadth, because a ban specific to legal process would have been too narrow. The SCA involves a situation where companies are holding onto others' data. These companies may not have as strong an incentive to protect their users' data because it is not their own privacy interests at stake. So, Congress needed to address not only compelled disclosure but also voluntary disclosure, which is consistent with the broad ban it enacted.[62] In this way, Congress needed to ban voluntary disclosures; simply banning disclosure pursuant to legal process would have been insufficient.

Similarly, for reports submitted by companies to the Census Bureau, as described below, Congress enacted a broad ban covering voluntary and compelled disclosures when the government was holding

61. Wexler, *supra* note 2, at 2764.

62. Even under the SCA, senders and recipients are free to disclose their own communications as they wish, just like with one's own census reports or tax returns.

onto the reports. On the other hand, with respect to copies of reports possessed by the owner (the company submitting the report to the Census), there is no need for restrictions on voluntary disclosure because the owners can decide how to deal with their own privacy interests. Thus, the statute did not prohibit such voluntary disclosures. On the other hand, a provision limited to "immune from legal process" is inconsistent with the circumstances Congress faced when enacting the SCA, specifically, it would undermine the disclosure scheme Congress needed to create to ensure third-party privacy protection. The ban needed to reach voluntary disclosures also.

The framework provided by privilege and privacy laws maps convincingly onto the SCA context. A privilege prevents the disclosure or use of information in a litigation setting. Communications privilege, which protects from disclosure information communicated within a protected relationship (attorney-client, marital, etc.), is one subset of privileges. The SCA's disclosure ban is, in part, similar to a communications privilege because of the relationship between the online company and the user. For comparison, take the marital communication privilege, which protects confidential communications between spouses during a marriage. Suppose a husband tells his wife where the murder weapon is buried and, separately, tells his best friend. The husband cannot prevent the best friend from revealing the information, including if the police compel the friend through a grand jury subpoena to reveal it. On the other hand, the police, even if they would prefer to get the information from the wife, cannot compel the wife to reveal the information. The husband can invoke the communications privilege. The husband, though, cannot prevent the wife from revealing it voluntarily outside the litigation context (such as to her best friend). But he can prevent the wife from disclosing it voluntarily within a litigation context because he is the holder of the privilege. He can also waive the privilege and allow the wife to disclose the information in a litigation context.

Now, consider the SCA. The relationship is between the subscriber and the service provider. These communications cannot be disclosed by the service provider in a litigation context. Others with the information, such as the recipient (like the best friend above), can be compelled to disclose it in a litigation context. The subscriber can prevent the service provider from voluntarily disclosing it in the litigation context because he is the holder of the privilege. And the subscriber can waive the privilege and allow the service provider to disclose it in the litigation context through the consent exception. In sum, the SCA's disclosure ban is doing what communications privileges do: it

bars the compelled disclosure of certain communications from certain sources.

But laws and other rules can do more than create privileges. They can protect information outside the litigation context as well. Consider, for example, an attorney's duty of confidentiality. This duty prohibits an attorney from disclosing private client communications outside the litigation context, which is why it is not a "privilege." Similarly, the SCA also does more than create a privilege because it also stops the service provider from disclosing the information outside the litigation context as well. It creates a privacy right in addition to a privilege. This distinction is key because it explains why sometimes specific words such as "immune from legal process" are appropriate, such as when Congress is only concerned about the litigation context and only wants to create a privilege, and why sometimes broader bans are necessary, such as when Congress wants to control disclosure outside the litigation context as well. That is what Congress did with the SCA's broad disclosure ban. The lack of certain terms like "immune from legal process" is a function of the breadth of the ban, which covers voluntary and compelled disclosures in a variety of contexts.

Because there is no ambiguity in the SCA, no canon of construction—like the presumption against privileges—is needed. The disclosure ban prohibits compelled disclosures except for governmental subpoenas and search warrants, as specified in the statute.

D. Wexler's Canon of Construction Only Can Apply During Ambiguity

The unambiguous nature of the disclosure ban brings an end to the statutory interpretation and the end of the legal analysis.[63] The Supreme Court "has explained many times over many years that, when the meaning of the statute's terms is plain, [the Court's] job is at an end. The people are entitled to rely on the law as written, without fearing that courts might disregard its plain terms based on some extratextual consideration."[64] Canons of construction, such as a pre-

63. *See* BedRoc Ltd. v. United States, 541 U.S. 176, 183 (2004) (citations omitted) (stating that the court "begins with the statutory text, and ends there as well if the text is unambiguous").

64. Bostock v. Clayton County, 140 S. Ct. 1731, 1749 (2020). *See also* Sandoz, Inc. v. Leavitt, 427 F. Supp. 2d 29, 36 n.5 (D.D.C. 2006) ("This argument would quickly fail, however, because the court will not engage in an analysis of legislative intent or employ any other cannons of statutory construction when the statute itself is unambiguous.").

sumption, are not used when the statute's term is plain.[65] Similarly, Wexler's presumption against privileges canon should not be used in the context of the unambiguous disclosure ban.

Typically, courts look at the plain text of the statute and decide whether there is ambiguity.[66] If there is none, that is the end. If there are two plausible interpretations, then courts may rely on a canon of construction to resolve the ambiguity. Application of the canon allows the court to pick one plausible interpretation over others in a non-arbitrary way.

Wexler's approach proceeds in the opposite way. Wexler advocates applying her presumption against privileges—a canon of construction—first, without determining whether the statute is ambiguous. Then, per Wexler's canon, because the statute does not contain certain words, it is ambiguous. According to Wexler, courts should once again apply the same canon to resolve this ambiguity by picking the interpretation allowing compulsory process.

There is a logical problem and a legal problem with using a canon to discover statutory ambiguity, as Wexler does. The logical problem is that Wexler's approach requires reading the disclosure ban as broad and narrow at the same time. Typically, the presumption would be used to resolve pre-existing ambiguity in the statutory text about whether the statute is broad (banning subpoenas) or narrow (allowing subpoenas). It would resolve that ambiguity in favor of the narrow reading. Wexler's claim is not that the statute is ambiguous in its breadth. Under Wexler's approach, the ban must be broad for the presumption against privileges to apply. It is a broad ban that creates privileges, such that the presumption would come into play. At the same time, the ban must be narrow to allow for defense subpoenas as Wexler advocates. This logical inconsistency exists because, as noted above, Wexler's approach requires using her presumption canon to discover ambiguity and then resolve that same ambiguity, rather than simply resolve an ambiguity that exists.

The legal problem is that the Supreme Court has rejected Wexler's approach in the context of similar canons of construction. *F.A.A. v. Cooper*,[67] for example, concerned the canon that requires an unmis-

65. Caminetti v. United States, 242 U.S. 470, 485 (1917) ("Where the language is plain and admits of no more than one meaning, the duty of interpretation does not arise, and the rules which are to aid doubtful meanings need no discussion.") (citing Hamilton v. Rathbone, 175 U.S. 414 (1899)).

66. *See* FAA v. Cooper, 566 U.S. 284, 290 (2012) (explaining that the canon of construction regarding waiver of sovereign immunity applies during statutory ambiguity).

67. *Id.*

takable statutory expression of congressional intent to waive the government's sovereign immunity.[68] This canon presumes Congress did not waive sovereign immunity unless unequivocally expressed. The presumption against privileges, according to Wexler, similarly requires presuming Congress did not ban certain disclosures unless unequivocally expressed. But as the Supreme Court explained in *Cooper*, the canon only applied when there was an ambiguity in the statute.[69] The Court also cautioned against finding ambiguity where none existed. It explained that "Congress need not state its intent in any particular way. We have never required that Congress use magic words."[70] Wexler is making the same mistake by requiring Congress to have used certain words, rather than using the canon as "a tool for interpreting the law" when the traditional tool of relying on the statute's text and structure does not provide a clear answer.

Similarly, consider the canon of the presumption against extraterritoriality. Like the presumption against privileges, the principle that acts of Congress do not apply extraterritorially is a "canon of construction, or a presumption about a statute's meaning."[71] Courts presume a statute is concerned with domestic application "unless there is the affirmative intention of the Congress clearly expressed" to give a statute extraterritorial effect.[72] The statute must give a "clear indication" of an extraterritorial application.[73]

Yet, even then, courts have not required any specific language as evidence of "clear indication." The statute does not need to say, "This law applies extraterritorially."[74] Rather, courts look to the text, structure, purpose, and "all available evidence"[75] of the statute to determine whether Congress gave an "affirmative indication" of extraterritorial application.[76] The Second Circuit, for example, held a "clear and affirmative indication" was present in a statute "criminalizing travel in foreign commerce undertaken with the intent to commit sexual acts with minors that "'would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdic-

68. *See id.* at 290–91.

69. *Id.* at 291.

70. *Id*.

71. Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 255 (2010).

72. EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991).

73. *Morrison*, 561 U.S. at 255.

74. *Id.* at 265 (stating that statute does not need to say "this law applies abroad").

75. United States v. Weingarten, 632 F.3d 60, 65 (2d Cir. 2011) (quoting Sale v. Haitian Ctrs. Council, Inc., 509 U.S. 155, 177).

76. *See Microsoft*, 829 F.3d at 211. *See also Morrison*, 561 U.S. at 265 ("Assuredly context can be considered as well.").

tion of the United States.'"[77] The focus of the law was the travel in foreign commerce, which went "to the heart of the statute's operative text."[78] Thus, the law had extraterritorial reach; a solely domestic application was not a permissible alternative.[79] The point is that in the analogous situation of the presumption against extraterritoriality, courts do not demand that Congress use a specific phrase but look to the overall text and structure of the law.

These cases reveal two relevant takeaways. First, canons, even those that require Congress to clearly express its intent, apply only to resolve ambiguity. Second, canons do not require statutes to use any specific words, even when they require Congress to clearly express its intent. Rather, even these canons are merely a tool of interpretation that apply once there is ambiguity about whether Congress did intend the outcome that is the subject of the canon. Applying these takeaways to the disclosure ban reveals that despite the presumption against privileges, the ban covers defense subpoenas for content. The broad ban and the rest of the statutory structure leave no ambiguity on that question.

E. The Interpretive Effect of Harsh Results

One of the main themes of Wexler's argument is that preventing defendants from compelling disclosures of content information from service providers creates significant harm to defendants, and therefore, the SCA must be interpreted to allow defendants to subpoena user content.[80] The argument could be that the harsh outcomes suggest the statute must yield to defense subpoenas because Congress could not have intended such a harsh result. As discussed in more detail in Part IV, though, defendants have several other avenues under the SCA to obtain communications. The harms do not appear to be nearly as broad as suggested. There also is nothing in the text, structure, purpose, or legislative history to suggest a congressional intent contrary to the plain text of the statute.[81]

77. *Weingarten*, 632 F.3d at 65 (quoting 18 U.S.C. § 2423(b)) (emphasis removed).

78. *See id.* at 66.

79. *See id.* at 65–66. *See also* Weiss v. Nat'l Westminster Bank PLC, 768 F.3d 202, 207 (2d Cir. 2014) (noting statute that made criminal an act "that would be a criminal violation if committed within the jurisdiction of the United States or of any State. . .[and] occur primarily outside the territorial jurisdiction of the United States" had extraterritorial application).

80. *See* Wexler, *supra* note 2, at 2738–40.

81. *See* United States v. Locke, 471 U.S. 84, 95–96 (1985) (noting Court could not go "behind the plain language" of the statute despite the harsh results because "neither appellees nor the dissenters have pointed to anything that so suggests" a contrary result and the legislative history does not suggest a contrary intent).

II.
The Supreme Court's Approach to Disclosure Bans

This Part examines three cases in which the Supreme Court interpreted discovery disclosure bans in other statutes, referred to by Wexler as the "trilogy."[82] Wexler argues that in this trilogy, the Supreme Court created a special rule of statutory interpretation in disclosure ban cases.[83] Drawing on statements in these cases about strictly construing statutory privileges, the argument is that these cases have imposed a "clear statement rule" that requires statutory disclosure bans to specifically and clearly ban legal process, such as by explicitly stating that the information is "privileged" or "immune from legal process," or by using other similar language.[84] Under this theory, a broad disclosure ban like the SCA's, even if it textually covers legal process, cannot be interpreted to ban compelled disclosures.[85] As this Part explains, this Supreme Court trilogy held exactly the opposite—that Congress does not need to use certain words or explicitly state a ban on disclosures pursuant to legal process.

A. St. Regis Paper Company v. United States

The first case in this trilogy is *St. Regis Paper Co. v. United States*.[86] St. Regis Paper Company had prepared and submitted a report to the Census Bureau that contained the company's business information.[87] It kept a copy of the report for its own records. The company refused a Federal Trade Commission order compelling it to produce the reports, arguing section 9 of the Census Act banned disclosure of the reports in its possession.

The Supreme Court held that section 9 did not prohibit disclosure of the reports in St. Regis' possession because the statute concerned only disclosures of reports held by the government.[88] The question was whether the statutory ban should be *expanded* by the Court to cover a business's copy due to policy concerns—namely, to encourage frank and efficient communications between businesses and the Census Bureau and to hold the Bureau to its promises to keep the reports confidential.[89] The *St. Regis* majority rejected these extratex-

82. Wexler, *supra* note 2, at 2765.
83. *See id.*
84. *See id.* at 2765–66.
85. *See id.* at 2775.
86. 368 U.S. 208 (1961).
87. *Id.* at 215.
88. *Id.* at 217–18.
89. *Id.*

tual considerations, explaining that these considerations could not "extend the coverage of the Act."[90]

The suggestion that *St. Regis* established a "clear statement rule" requiring Congress to explicitly ban compelled disclosures is a surprising reading of this case.[91] The parties,[92] the lower courts,[93] and the Supreme Court[94] all agreed section 9 banned compelled disclosures of reports in the hands of the Census Bureau. Yet, section 9 has no explicit language about legal process. That means a statute can ban disclosure pursuant to legal process without using specific terms. Rather, the plain reading of section 9, consistent with its purpose, was that it banned compelled disclosures of reports possessed by the government.[95]

---

90. *Id.* at 218.

91. *See* Wexler, *supra* note 2, at 2757, 2760.

92. For example, the Solicitor General's brief noted that "reports made to the Census Bureau under compulsion of law are privileged, while in its possession, against subpoena or other legal process" and "are not subject to legal process." Brief for the United States at 29, *St. Regis Paper*, 368 U.S. 208 (No. 61-47). St. Regis argued reports in the company's possession "are entitled to the same confidential treatment as the original copies of census reports furnished to the Bureau" and "not amenable to Commission investigative process." *See* Brief of Petitioner St. Regis Paper Company at 12, *St. Regis Paper*, 368 U.S. 208 (No. 61-47).

93. FTC v. Dilger, 276 F.2d 739, 740, 744 (7th Cir. 1960) (holding section 9's privilege extended to reports in the company's possession); *United States v. St. Regis Paper Co.*, 285 F.2d 607, 613–14 (2d Cir. 1960), *aff'd*, *St. Regis Paper*, 368 U.S. 208 (recognizing section 9 prohibited the Bureau from disclosing the reports, just like tax laws prohibit compelled disclosures of tax returns by the government). *See also* United States v. Bethlehem Steel Corp., 21 F.R.D. 568, 569-70 (S.D.N.Y. 1958) (holding section 9's privilege banned compelled disclosure of reports held by the Census).

94. *St. Regis*, 368 U.S. at 217–19 (noting the "prohibitions against disclosure" run only against officials and citing favorably to tax cases holding the government is prohibited from disclosing tax returns pursuant to legal process). Professor Wexler suggests *St. Regis* actually left open the question of whether reports possessed by the Census Bureau were subject to compulsory process, and the issue was finally decided in *Baldridge*. *See Wexler*, supra note 2, at 2761 n.249. This reading of the two cases seems mistaken. *Baldridge*, as discussed below, concerned raw data (not reports) possessed by the Census, which implicated different disclosure bans found in sections 8 and 9. The whole question in *St. Regis* was whether to "extend" the protections afforded to reports in the possession of the Census Bureau, meaning that the reports held by the Census Bureau were protected from discovery.

95. Like the Census Act, the tax return confidentiality provisions banned disclosures by government employees but did not address returns possessed by taxpayers. *See* Internal Revenue Code of 1954, Pub. L. No. 83-591, § 6103, 68A Stat. 3, 753 (current version at I.R.C. § 6103) ("except as hereinafter provided in this section, they shall be open to inspection only upon order of the President and under rules and regulations prescribed by Secretary. . .and approved by the President"); *Id.* § 7213, 68A Stat. at 855 (current version at I.R.C. § 7213) ("It shall be unlawful for any officer or employee of the United States to divulge or make known in any manner whatever not provided by law to any person [tax information]."). The provisions were

Undoubtedly, the Court in *St. Regis* established a rule that statutory disclosure bans must be "strictly construed." But this sentence was a rejection of expanding a statute beyond its terms due to policy concerns, as *St. Regis* had suggested. The D.C. Circuit explained as much in analyzing *St. Regis*: "The Court's [strict construction] statement . . . was made in the course of rejecting an argument for expanding the reach of a statutory privilege beyond its terms. The Court declined to do so, noting that 'we cannot rewrite the Census Act.'"[96]

St. Regis could not have established Wexler's rule requiring that a statute use certain words (like "immune from legal process") to ban compelled disclosures; section 9 was thought to ban compulsory process yet contained no "clear statement" about doing so.

B. Baldridge v. Shapiro

Baldridge v. Shapiro[97] also concerned disclosures under the Census Act. Section 9(a) contained identical language as in the *St. Regis* case. Section 8(b), which is referenced in section 9(a), reads as follows: "the Secretary [of Commerce] may furnish copies of tabulations and other statistical materials which do not disclose the information reported by, or on behalf of, any particular respondent. . ."[98]

The *Baldridge* Court recognized that a statute granting a privilege must be "strictly construed."[99] Still, the Court concluded Sections 8(b) and 9(a) did create a privilege and its language "embod[ied] explicit congressional intent to preclude *all* disclosure of raw census data reported by or on behalf of individuals."[100] This case alone is a significant barrier to Wexler's argument that under Supreme Court doctrine, the SCA's disclosure ban cannot create a privilege because it "never mentions privilege, discovery, subpoenas, courts orders, admis-

---

read to bar compulsory process, *see* Kingsley v. Delaware, L&W R.R. Co., 20 F.R.D. 156, 159 (S.D.N.Y. 1957) (collecting cases), even though, again, they contained no explicit terms and one of the confidentiality provisions was similar to the SCA's. The *St. Regis* Court cited favorably to this line of cases. *See St. Regis*, 368 U.S. at 219 n.10 and accompanying text (citing, as an example, United States v. O'Mara, 122 F. Supp. 399 (D.D.C. 1954)).

96. In re England, 375 F.3d 1169, 1180 n.2 (D.C. Cir. 2004).

97. 455 U.S. 345 (1982).

98. Act of Oct. 17, 1976, Pub. L. 94-521, § 6(a), 90 Stat. 2459, 2460 (codified as amended at 13 U.S.C. § 8(b)).

99. *Baldrige*, 455 U.S. at 360. The Court even recognized the harsh results of its ruling—"This is not to say that the city of Denver does not also have important reasons for requesting the raw census data for purposes of its civil suit."— but concluded it could not alter the statutory language that created a privilege. *Id.* at 362.

100. *Id.* at 361.

sibility, or any even remotely similar language."[101] The *Baldridge* Court found a privilege in a statute that used none of this language.

Baldridge rejected the kind of clear statement rule suggested by Wexler. At oral argument, George Cerrone, counsel for Denver, made the same argument that Wexler does: Congress knows how to ban disclosures pursuant to compulsory process and does so by using specific language.[102] It used specific language in the latter part of section 9(a) concerning census reports ("immune from legal process") but did not use this specific language in the main part of section 9(a) concerning raw data. Thus, Cerrone argued, Congress did not intend to ban compelled disclosures for raw data.[103] In fact, this argument was repeatedly addressed in oral argument. Justice O'Connor asked Elliot Schulder, counsel for the federal government, about the fact that here, Congress did not expressly prohibit discovery disclosures, "although it does in many instances."[104] Schulder responded that this argument would mean census reports in the hands of the Census Bureau were discoverable under section 9(a), because section 9(a) also did not expressly prohibit discovery disclosures. This outcome was plainly inconsistent with the Court's analysis in *St. Regis*.[105] At the end, in its written opinion, the Court enforced the broad ban as written despite its lack of specific language. The Court necessarily rejected the constricted reading that would require Congress to use certain words to ban compelled disclosures.

Recognizing the impediment that *Baldridge* presents, Wexler alternatively suggests that courts can imply a privilege—meaning a statute can ban compelled disclosures even when it does not use specific words referencing legal process. According to Wexler, courts can imply a privilege only in the "narrow" circumstance where a broad disclosure ban has "no enumerated exceptions other than to return information to the source from whence it came."[106] Yet, the *Baldridge* Court did not rely on the lack of exceptions; it never even mentioned

101. Wexler, *supra* note 2, at 2775.

102. *Id.* at 2763 ("Congress knows how to write an express statutory privilege when it wants to" and then citing the portion of section 9(a) concerning census reports in private hands); Oral Argument at 1:12:56, *Baldrige*, 455 U.S. 345 (No. 80-1436), https://www.oyez.org/cases/1981/80-1436 [https://perma.cc/TDM6-ZSKW] (Cerrone: "I will address the plain language of the statute, Justice Stevens, by saying that there is nothing in that statute that is applicable to a court except how Congress amended the Act with respect to respondent retaining copies, and that is the only place where there is any mention as to restrictions on judicial disclosure.").

103. *Id.*

104. *Id.* at 1:31:02–1:31:08

105. *Id.* at 1:31:08.

106. Wexler, *supra* note 2, at 2769, 2771.

exceptions. It relied generally on the breadth of the ban's text and the statute's purpose and legislative history. Similarly, at the time of *St. Regis*, for example, section 8 contained a plethora of exceptions.[107] Yet, as described above, the disclosure ban on census reports had been read to create a privilege. The same is true of the tax return confidentiality provisions mentioned in *St. Regis*—they too had a plethora of exceptions but had been read to create a privilege.[108] The Court left these cases undisturbed.

This "exceptions" approach also leaves several questions unanswered. The scope of the supposed rule remains undefined: how many exceptions are too many? One? Two? Three? Does the nature of the exception matter? What kinds of exceptions are allowed? What about exceptions that are necessary? Wexler concedes that necessary exceptions are allowed,[109] but how would a court even decide what exception is necessary? And necessary for what—the statute's purpose, a broader societal goal, public health and safety, or something else? And what would give a court authority to evaluate an exception's "necessity," which ultimately is a policy issue? This approach creates broad uncertainty. Yet, the purpose of disclosure bans—especially the SCA's—is to create certainty to encourage what are seen as socially beneficial communications such as between Internet users or between an individual and the Census Bureau.

As noted above, exceptions can be a signal of the breadth of a disclosure ban. A broader ban—one that covers all kinds of disclosures—needs more exceptions. A narrow ban that, for example, only covered disclosures of a certain report to a certain person in certain circumstances would not need any exceptions. Yet, under Wexler's "exceptions" approach, a broader ban with exceptions oddly would be read *more* narrowly because the presence of exceptions would mean compelled disclosures were allowed.

After *Baldridge*, Congress amended the Census Act to create a comprehensive disclosure scheme that allowed the disclosure of some

---

107. Act of Aug. 31, 1954, Pub. L. 83-740, § 8, 68 Stat. 1012, 1013 (current version at 13 U.S.C. § 8). (allowing disclosure of data and reports to states, courts, and individuals in various circumstances); Act of Aug. 28, 1957, Pub. L. 85-207, sec. 4, § 8, 71 Stat. 481, 481 (current version at 13 U.S.C. § 8). *See also* Wexler, *supra* note 2, at 2761 & n.245.

108. Internal Revenue Code of 1954, Pub. L. No. 83-591, §§ 6103, 7213(a), 68A Stat. 3, 753 (current version at I.R.C. §§ 6103, 7213(a)) (broadly allowing disclosures pursuant to rules established by the Secretary of the Treasury; allowing disclosures to states and congressional committees), 855 (broadly allowing disclosures "as provided by law").

109. Wexler, *supra* note 2.

raw census data to localities.[110] Congress imposed a variety of secrecy requirements as part of this process. Here, too, Congress can amend the SCA to develop a comprehensive disclosure scheme for non-governmental legal process, just as it has done for governmental legal process. Congress can balance privacy interests with disclosure interests, and it can create procedures that will ensure defendants can access content while giving confidence to subscribers about the privacy of their data. Having courts create this scheme is not the answer.

C. Pierce County v. Guillen

Finally, in the third of the trilogy cases, *Pierce County v. Guillen*,[111] the Court again followed the text of the statute as written. Federal law funded state highway improvements but required states to conduct engineering surveys to identify hazards that needed to be fixed.[112] States worried that these surveys, if non-confidential, could increase states' risk of liability for accidents that occurred at hazards before states could fix them.[113] Congress enacted a confidentiality provision requiring that information collected for the program "shall not be subject to discovery."[114] The issue in *Pierce County* was whether plaintiffs could obtain certain highway accident reports in their tort lawsuit. These accident reports had been created by the county sheriff for purposes unrelated to the funding program but then gathered by another agency as part of the funding program.[115] The Court concluded the provision was ambiguous as to the accident reports held by this other agency; it noted that the federal government's and plaintiff's readings were plausible.[116] The Court applied the *St. Regis* canon of construction that privileges should be strictly construed to resolve this ambiguity. It adopted the federal government's interpretation, which took a narrower view of the privilege.[117]

---

110. Census Address List Improvement Act of 1994, Pub. L. 103-430, § 2(a), 1108 Stat. 4393, 4393 (codified at 13 U.S.C. § 16).

111. Pierce Cty. v. Guillen, 537 U.S. 129 (2003).

112. *Id.* at 133.

113. *Id.* at 134.

114. *Id.* at 135–36.

115. *Id.* at 143.

116. *Id.* at 145.

117. *Id.* Wexler claims that *Pierce* "is consistent with a requirement that statutory privileges must be express." Wexler, *supra* note 2, at 2765. It is difficult to see how. *Pierce* said nothing and alluded to nothing about what makes a statutory privilege; that was not at issue. The only question was the scope of the privilege. Even Professor Wexler later admits the case "does not clarify whether such express language is necessary to create a privilege." *Id*. at 2766.

The trilogy of Supreme Court cases sets out what it means to "strictly construe" a statutory privilege. First, per *St. Regis*, courts should not expand the statutory privilege beyond its text for policy reasons. Second, per *Pierce*, if a statute is ambiguous and equally susceptible to two possible meanings, the presumption against privilege can resolve the tie in favor of disclosure. The strict construction rule requires no more. *Baldridge* showed that Congress need not use any specific or explicit words to create a privilege. *Pierce* made clear that the strict construction rule is cabined by the text of the statute and the rule's implementation cannot contradict the text.

D. Circuit Court Cases

The case that most explicitly rejects Wexler's argument is the D.C. Circuit's *In re England*,[118] authored by then-Judge John Roberts. Navy chaplains received promotions according to decisions made by "selection boards."[119] Certain chaplains sued, alleging discriminatory practices by these boards.[120] In language nearly identical to the SCA's, section 618(f) rendered board proceedings confidential.[121] Like Wexler's argument, the district court in *In re England* held section 618(f) "did not preclude disclosure of selection board proceedings through civil discovery, because Congress had not expressly addressed the question of such discovery in providing that board proceedings 'may not be disclosed.' "[122] The D.C. Circuit reversed.

Like any case involving statutory interpretation, the court "beg[a]n with the plain language of the statute" and read this language as commanding a ban on disclosure.[123] In so concluding, the court acknowledged statutes that create a privilege must be "strictly construed" but this presumption could not "justify departing from those plain terms pursuant to a judicially-crafted exception."[124]

Next, the court explained that the "except" clause further supported rejecting judicially-created exceptions. Because Congress specified certain exceptions—and did not specify an exception for disclosure in discovery—the court was "reluctant to imply an additional exception for that purpose."[125] Also, the nature of the excep-

118. 375 F.3d 1169 (D.C. Cir. 2004).
119. *Id.* at 1170.
120. *Id.*
121. *Id.*
122. *Id.* at 1171; *see also* Chaplaincy of Full Gospel Churches v. Johnson, 217 F.R.D. 250, 260 (D.D.C. 2003).
123. *In re England*, 375 F.3d at 1170.
124. *Id.*
125. *Id.* at 1178.

tions spoke to the breadth of the ban. The ban on disclosure was so "broad and absolute" that Congress needed to create basic and obviously necessary exceptions.[126] Similarly, with the SCA, as described above, the narrow statutory exceptions were those necessary for the functioning of the service and public safety.

At this point, the *In re England* court concluded that the judicial inquiry was "complete" because the terms of the statute were unambiguous.[127] But what about the district court's assertion that the statute did not contain specific language barring discovery? The D.C. Circuit rejected this approach because a statute written in "broad, sweeping language" should be given "broad, sweeping application."[128] The D.C. Circuit also noted that the Supreme Court rejected such an approach in *Baldridge*, which held that the "unambiguous language" of the confidentiality provision barred discovery—even though it contained no specific mention of discovery or privilege.[129] Other Supreme Court, federal appellate court, and federal district court cases have analyzed broad disclosure bans and similarly interpreted them to prohibit discovery disclosures despite the lack of specific language.[130]

Two other circuit cases are worth mentioning because Wexler relies heavily on them: a 1989 Eleventh Circuit case and an almost identical 1992 Ninth Circuit case.[131] Both cases concerned disclosure bans for information obtained from undocumented immigrants "to assure applicants that the legalization process is serious, and not a ruse to invite undocumented aliens to come forward only to be snared by INS."[132] Both cases held that the statutory provisions did not ban dis-

126. *Id.* at 1177.

127. *Id.* at 1178 (quoting Adams Fruit Co. v. Barrett, 494 U.S. 638, 642 (1990)).

128. *Id.* at 1179 (quoting *Consumer Elecs. Ass'n*, 347 F.3d at 298).

129. *Id.* (quoting *St. Regis Paper*, 455 U.S. at 355).

130. *See, e.g.*, CIA v. Sims, 471 U.S. 159 (1985); Cazorla v. Koch Foods of Miss., LLC, 838 F.3d 540, 551 (5th Cir. 2016) ("But as a purely textual matter, it is unclear why a provision broadly barring any "disclosure" would have to specify "including in discovery" in order to have effect."); Lessner v. U.S. Dep't of Com. 827 F.2d 1333, 1337, 1340 (9th Cir. 1987); EEOC v. SOL Mexican Grill, LLC, No. CV 18-2227, 2019 WL 2896933, at *3 (D.D.C. June 11, 2019); Chowdhury v. Nw. Airlines Corp., 226 F.R.D. 608, 610–11 (N.D. Cal. 2004).

131. Zambrano v. INS, 972 F.2d 1122 (9th Cir. 1992); In re Nelson, 873 F.2d 1396 (11th Cir. 1989). In footnote 184, Professor Wexler also cites a string of district court opinions. Many of these cases relied on the language of *Friedman*, *Freeman*, and *Laxalt* – the three D.C. Circuit cases that *In re England* explained could *not* be read to impose an explicitness requirement. Others in the string cite concern the same issue about disclosure to class counsel found in the Ninth and Eleventh Circuit cases. *See* Wexler, *supra* note 2, at 2751 n.184.

132. H.R. REP. NO. 99-682, pt. 1, at 73 (1978), *as reprinted in* 1986 U.S.C.C.A.N. 5649, 5677.

closures to attorneys representing those undocumented immigrants.[133] These cases are difficult to assess because the analysis is perfunctory; neither opinion contains any analysis of the statutory text. The entirety of the Eleventh Circuit's analysis consists of three sentences.[134] Both opinions relied heavily on the D.C. Circuit's opinion in *Freeman v. Seligman*, which they read as suggesting Congress must explicitly ban court disclosures.[135] But the D.C. Circuit later in *In re England* clarified that such a reading of *Freeman* was incorrect.[136] Other than that, the Eleventh Circuit relied on a single sentence from the House Report about providing an assurance to applicants that is quoted above.[137] And the Ninth Circuit case relied on the Eleventh Circuit's conclusion.[138]

Both cases presented fairly unique circumstances that make them poorly suited to extrapolate to the SCA disclosure ban, especially given the weight of contrary precedent. In the immigration cases, the applicants sought the disclosure of their own information to themselves that was being protected for their own benefit. Regardless of privilege, they were entitled to their own information. They simply sought a return of their own information. The Eleventh Circuit's brief opinion, for example, focused on the fact that the district court's discovery order limited the disclosure to the applicants' attorneys. This limitation is consistent with the disclosure constituting a return of information to the applicants (or their agents), rather than a determination about the scope of the statutory privilege.

Another way to look at what occurred is as a limited waiver of privilege. In the Ninth and Eleventh Circuit cases, the applicants, through their attorneys acting as their agents, waived their privilege for the limited purpose of obtaining their own information.[139] The applicants submitted their personal information to the government. This

133. *See Zambrano*, 972 F.2d at 1125; *Nelson*, 873 F.2d at 1397.

134. *See Nelson*, 873 F.2d at 1397.

135. *See Zambrano*, 972 F.2d at 1125.

136. *See In re England*, 375 F.3d at 1179–80.

137. *See Nelson*, 873 F.2d at 1397.

138. *See Zambrano*, 972 F.2d at 1125–26. In the Ninth Circuit case, the provision was similar to the one analyzed in *Baldridge* so the court had to distinguish that case. It did so by making the same mistake Wexler makes and believing the *Baldridge* Court relied on the express exclusion provision (which it did not since that provision was limited to reports retained by businesses). *See id.* at 1122.

139. Whether the government agency also holds the privilege is beyond the scope of this Article but it likely is asserting the privilege on the holder's behalf (the applicant). *See* 2 EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE [EVIDENTIARY PRIVILEGES] § 6.12.3 (3d ed. 2017). In any case, any holder of a privilege can waive it as to their own information; consensus is not required. *See id*.

personal information was protected from disclosure, but the applicants were the holder of the privilege because they were the "intended beneficiary of the privilege."[140] The purpose of the disclosure ban was to protect the applicant's information, especially to encourage frank communication between the applicant and the government. Since they held the privilege, they could do a limited waiver to allow the disclosure to themselves. The SCA also allows for this kind of limited waiver; a user can provide consent for the disclosure of content by the online company. But that is different than a defendant compelling the online company to produce information about a third-party user.

Similarly, in the telegram era, as discussed below, legal scholars debated whether telegrams were privileged. But even if they were privileged, it was accepted that the privilege could be waived by those entitled to their information—the sender and the receiver.[141] When the sender or receiver hauled the telegraph company into court because of a delay or failure in transmitting a message, as happened with some frequency, they could waive any privileges and introduce the telegrams into evidence despite privileges created by statute.[142]

III.
Compelled Disclosure of Telegrams

Over a century ago, various states passed laws banning the disclosure of telegrams by telegraph companies. Courts sometimes interpreted the scope of these bans and, according to Wexler, required the telegram disclosure bans to explicitly ban legal process.[143] A key aspect of Wexler's argument is the assertion that courts' previous interpretation of telegram statutes can be directly mapped onto the SCA. The instinct behind this thought is reasonable: telegram laws contained disclosure bans like the SCA and both dealt with user communications stored by a service provider. However, a proper analysis of the courts' application of telegram statutes, as discussed below, shows that courts applied the plain meaning of the statutes, which varied

140. *Id.* § 6.12.1 ("In particular, in the United States, the assumption is that any privilege, including the clergy-penitent privilege, can be waived.").

141. *See, e.g.*, T.M. Cooley, *Inviolability of Telegraphic Correspondence*, 18 Am. L. Reg. 65, 66 (1879) ("The privilege of secrecy is the privilege of the parties, and would necessarily be waived by either if he were to complain of the company's action.").

142. *See, e.g.*, Massengale v. Western Union, 17 Mo. App. 257, 258-59 (Mo. Ct. App. 1885) (noting copies of the telegrams were introduced at trial in negligence suit alleging error by telegraph company); Woods & Bradley v. Frank Miller & Co., 7 N.W. 484, 484–85 (Iowa 1880) (noting parties to a telegraph message can always introduce the telegram as evidence in a dispute between them).

143. Wexler, *supra* note 2, at 16.

from state to state. For example, some of these laws explicitly contained exceptions for disclosures as part of court proceedings, and courts dutifully applied these exceptions to allow subpoenas. This approach is consistent with current interpretation of the SCA and forecloses the application of additional canons of interpretation. Before getting to the specific statutes, this Part describes the privileged nature of postal mail, which provides the necessary context for understanding these early courts' discussions of whether telegrams were similarly privileged.

A. A Brief History of the Inviolability of Postal Mail

Towards the end of the nineteenth century, scholars and judges were engaged in a vigorous debate about whether telegrams were "privileged" and "inviolable" like postal mail. Postal mail was seen as private, secret, and privileged. As other scholars have detailed, by the early 1770s, sealed correspondence was the "principal means by which the [American] rebels communicated with those from other colonies."[144] The rebels became concerned that the British post office would open and read their correspondence to determine who was a "traitor"—especially because much of what they were doing *was* treasonous.[145] "Confidentiality of correspondence was thus a significant factor motivating the establishment of the separate 'constitutional post.'"[146] The Founders included as one of Congress's enumerated Article I powers the establishment of the postal service. William Goddard, a newspaperman, had created a private postal network that the Second Continental Congress adopted and turned into the U.S. postal service.[147] One of Goddard's proposed "model rules" for a postal network was "[t]hat the several mails shall be under lock and key, and liable to the inspection of no person but the respective Postmasters to whom directed, who shall be under oath for the faithful discharge of the trust reposed in them."[148] Thus, the "principle of confidentiality of the mail" was baked into the American postal network at its founding

144. Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 563 (2007).
145. *Id.*
146. *Id.* at 564.
147. *Id.* at 564-65.
148. William Goddard, Proposal for Establishing an American Post Office (July 2, 1774), *reprinted in* 4 AMERICAN ARCHIVES 500 (Peter Force ed., 1837), https://archive.org/details/americanarchives41forc/page/n317/mode/2up [https://perma.cc/9NE2-R5UJ].

and this network sought to "preserve the inviolability of the contents of private communications."[149]

Over the years, the federal government promulgated laws and regulations to codify these understandings. Benjamin Franklin, as deputy postmaster, created a regulation requiring all postmasters "to subscribe to an oath that they would not tamper with the mail."[150] In October 1782, the Continental Congress passed a postal ordinance requiring that postal employees "shall not knowingly or willingly open. . .any letter. . . except by the consent of the person or persons by or to whom the same shall be delivered or directed, or by an express warrant under the hand of the President of the Congress of these United States. . . or of the chief executive officer of one of the said states, for that purpose, or except in such other cases wherein he shall be authorized so to do by this ordinance."[151] On March 3, 1825, Congress enacted comprehensive postal regulations that prohibited postal employees from detaining, delaying, or opening letters and made it unlawful for any person to take or open any letter before it was delivered "with a design to obstruct the correspondence, to pry into another's business or secrets."[152] Both laws have continued in some form to present day.[153]

In 1878, the Supreme Court finally held that sealed postal mail was "privileged" in the sense that it was protected under the Fourth Amendment the same as papers "in one's own household" even though it had been transferred into the custody of the post office.[154] Postal mail could only be opened and examined upon the issuance of a warrant that met the requirements of the Fourth Amendment.[155]

By the time the telegraph became embedded in American life, it was understood that postal mail in the hands of the post office was "inviolable." Courts and legal commentators varied on the reasons why: due to the federal and state constitutional prohibitions on unreasonable searches, the acts of Congress cited above, or a general sense of fairness that the government could not contravene the confidence it had invited among the public in the secrecy of the mail. Michigan Supreme Court Chief Justice Thomas Cooley, one of the most respected legal scholars of the era, wrote the "importance of public

149. Desai, *supra* note 144, at 565.
150. *Id.* at 563.
151. *Id.* at 566 n.54.
152. Act of March 3, 1825, ch. LXIV, §§ 21-22, 4 Stat. 102, 107-09 (eventually codified at 46 Rev. Stat. §§ 3891-92 (2d ed., 1878)).
153. *See* 18 U.S.C. §§ 1702, 1703(a).
154. Ex Parte Jackson, 96 U.S. 727, 733 (1878).
155. *Id.*

confidence in the inviolability of correspondence through the post-office cannot well be overrated; and the proposition to permit letters to be opened, at the discretion of a ministerial officer, would excite general indignation."[156] Henry Hitchcock, another legal scholar from the era, acknowledged "the inviolability (except upon lawful warrant) of sealed letters intrusted to the Government" because a disclosure otherwise would be an unreasonable search and seizure.[157]

B. The Debate Over Whether Telegrams Were Privileged Like Postal Mail

As noted by Wexler, courts during the telegram era discussed whether telegrams were "privileged." But context is important; this discussion about privilege was about whether telegrams were privileged not due to any statute but because they were used for confidential communications. By 1875, the telegraph had become "one of the necessities of commerce,"[158] and "transmitted the desires, the purposes, the transactions of every class."[159] A debate ensued about whether this private correspondence should be treated as "inviolable" like postal correspondence.[160] Chief Justice Cooley was the main pro-

156. THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 306 n.2 (Boston, Little, Brown, & Co. 1868). For examples of Judge Cooley's prominence, *see, e.g.*, 44 CONG. REC. 602 (House, Jan. 12, 1877) (noting Chief Justice Cooley's opinions on this topic were "weighty words this House has been so solemnly conjured to carefully consider"); Warren v. State, 72 So. 624 (Ala. 1916) (calling Chief Justice Cooley an "eminent authority"); McKinley v. City of Chicago, 16 N.E.2d 727 (Ill. 1938) (same); Alphin v. Wade, 116 S.W. 667 (Ark. 1909) (similar); State v. Moran, 182 P. 927 (Nev. 1919) ("eminent authority on constitutional law"). *See also* Note, *The Right to Privacy in the Nineteenth Century*, 94 HARV. L. REV. 1892, 1896 (1981) (calling Chief Justice Cooley "a leading constitutional authority"); Michael J. Pallamary, *Revisiting Cooley*, THE AM. SURVEYOR (Aug./Sept. 2015) (identifying Chief Justice Cooley as "one of the best known judges in the country" and his 1868 treatise on constitutional limitations as "one of the most the important treatises on constitutional law").

157. Henry Hitchcock, *The Inviolability of Telegrams*, 5 S. L. REV. (NEW SERIES) 492–93 (1879). Until 1961, the Fourth Amendment only applied to the federal government, but most states had similar bans against unreasonable searches in their state constitutions. *See* Mapp v. Ohio, 367 U.S. 643 (1961).

158. Pensacola Tel. Co. v. Western Union Tel. Co., 96 U.S. 9 (1877).

159. Hitchcock, *supra* note 157, at 484.

160. *See, e.g.*, JOHN ORDRONAUX. CONSTITUTIONAL LEGISLATION IN THE UNITED STATES: ITS ORIGIN, AND APPLICATION TO THE RELATIVE POWERS OF CONGRESS, AND OF STATE LEGISLATURES 249 (T. & J.W. Johnson & Co., 1891). ("The question whether telegraphic messages, not being sealed, are in the nature of private correspondence, and to be protected, like letters in the mail, against compulsory production in the hands of a telegraph company, has given rise to many contradictory opinions as to their proper legal status under the fourth amendment to the Constitution.").

ponent of doing so. His view was independent of any specific statute that could have made telegraphs privileged.[161] Rather, for Chief Justice Cooley, the "general principles which are the animating spirit of constitutional law" required maintaining the privacy of telegraphic correspondence just as they did for sealed mail correspondence or an individual's private papers.[162] Chief Justice Cooley noted that "secrecy of the mails" had been "protected from the earliest days" and "admit of no exception."[163] And, like private mail, Chief Justice Cooley believed senders and receivers treated their telegrams as private correspondence.[164]

Courts and other commentators almost universally rejected Chief Justice Cooley's argument based primarily on a key distinction between mail and telegrams.[165] With respect to the mail, the government itself had invited the confidence of the public in accepting sealed letters and it would be "a breach of faith, shocking to the commonest sense of justice," to then turn around and breach that confidence by disclosing private correspondence using the government's own power through compulsory process.[166] The same was not true of the telegraph, which was operated by private companies.[167] Using compulsory process to compel the production of telegrams would not be a breach of the government's promises.[168] So, for example, in England telegrams were protected from compelled disclosure like the mail but that was because the English government had sole control over telegraphic communications, just like the mails.[169]

---

161. Cooley, *supra* note 40, at 67 ("In discussing this question it will be assumed that there is no express prohibition of law , and that if prohibited at all it is by the penalty which is imposed for voluntary disclosures. . .").

162. *Id.*

163. *Id.* at 69–70.

164. *Id.* at 66.

165. *See* Ex Parte Brown, 72 Mo. 83, 91 (1880); In re Storror, 63 F. 564, 566 (N.D. Cal. 1894); State v. Litchfield, 58 Me. 267, 269-70 (1870). Courts sometimes also relied on various other reasons that are outside the scope of this Article.

166. Hitchcock, *supra* note 157, at 492–93; ORDRONAUX, *supra* note 160, at 249; *Ex Parte Brown*, 72 Mo. at 91 ("On the other hand postal facilities were established by Congress; the mails are carried by the government through its own agents, and penal statutes protect communications sent through the mail. The entire postal system is under the control and management of the government.").

167. *See* Olmstead v. U.S., 277 U.S. 438, 464 (1928) (noting the mail was protected because the government controls and runs it but the same is not true of the telegraph and telephone).

168. Ex Parte Brown, 7 Mo.App. 484 (Mo. Ct. App. 1879).

169. *See* Hitchcock, *supra* note 157, at 492 n.5; 44 CONG. REC. 603 (House, Jan. 12, 1877) ("It must be remembered that in each of these cases [English cases in which postal operator was excused from producing telegrams] the witness was a government official, engaged in a department depending. . .upon an implied pledge of the confi-

This history provides the necessary context for discussions about the privileged nature of telegrams in the various court cases cited by Wexler. Lawyers and commentators back then were debating whether the privilege in the mail and potentially telegrams was *sui generis* because of "high public policy" favoring private correspondence or due to the "animating spirit" of state constitutions.[170] It had little to do with interpreting various state statutes concerning the disclosure of telegrams.

The next section discusses the state laws concerning disclosures of telegrams and court cases interpreting them to show that courts did not impose a so-called clear statement rule requiring an explicit mention of immunity from legal process. Accordingly, these courts do not appear to have implied exceptions for compelled disclosures into otherwise broad disclosure bans, as suggested by Wexler. Courts in the telegraph era interpreted disclosure bans the same way modern courts have, by applying the plain meaning of the text of these statutes.

C. Court Cases Interpreting Telegram Confidentiality Statutes

Until 1934, no federal law existed regarding the secrecy of telegrams.[171] As a federal matter, telegram companies were allowed to divulge communications as they saw fit. States, however, took varying approaches. As of 1879, eighteen out of thirty-eight states had no law restricting the disclosure of telegrams. The remaining states varied in their statutory language. One thing to remember is that there were only *five* cases reported nationally discussing whether states statutes barred discovery disclosures. With so few decisions, two of which were at the trial court level interpreting different statutes, it would be impossible to tease out any kind of a well-established approach during this era. There was no overarching approach, except courts uniformly rejected Chief Justice Cooley's view that telegrams, like the mail, were fully privileged under the constitution or as a matter of public

---

dence of the Crown. . .Hence there was a strong reason for the ground. . .,namely, the impolicy of the Crown—the only power which could compel its agent to disclose the messages in his possession—violating the confidence it had invited and the faith it had impliedly pledged in establishing its postal telegraph."). *See also* ORDRONAUX, *supra* note 160, at 249 (noting that to give telegrams full protection so they could never be produced, the telegraphic lines needed to be taken over by the government and made a part of the postal service).

170. Merchants' Nat. Bank of Wheeling v. First Nat. Bank of Wheeling, 7 W.Va. 544, 546–47 (1874) ("letters passing through the mails" are "protected for reason of high public policy").

171. Hitchcock, *supra* note 157, at 494; Desai, *supra* note 144, at 583; *In re Storror,* 63 F. at 566.

policy.[172] Even so, in looking through individual cases, the nineteenth-century courts do not appear to have relied on any clear statement rules about discovery bans.

Two states, Missouri and Indiana, had secrecy statutes that explicitly contained exceptions for disclosures to "courts of justice." So, the plain text of these two statutes allowed disclosures pursuant to legal process—and did not limit the kinds of allowable legal process. Courts at the time simply applied the plain text of these laws. For example, in the Missouri case *Ex parte Brown*,[173] a grand jury subpoena was issued to a telegraph employee to produce all telegrams on a certain topic. Citing the Missouri secrecy statute, the employee refused and was promptly held in contempt.[174] The secrecy statute did not contain an exception for disclosures to a "court of justice," however, a related criminal statute did contain such an exception.[175] In interpreting the civil statute, the Missouri Supreme Court understood it to contain an exception for compulsory process because of the related exception in the criminal statute. The court explained, "[I]n that exception [to a court of justice] we have a legislative recognition of the amenability of custodians of telegrams to a subpoena *duces tecum*, commanding their production."[176] It was harmonizing the two statutes. One can disagree with this approach to statutory interpretation. After all, the legislature knew how to write an exception for disclosures to courts when it wanted to and did not do so in the civil statute. But this disagreement is beside the point; the bigger point is that the court did not apply any sort of a presumption against privileges in interpreting the civil statute. It relied on the express exception for court disclosures. In fact, the lower court had used the kind of presumption proposed by Wexler; it had stated, "It is understood that there is always an exception in favor of legal process."[177] The Missouri Supreme Court did *not* adopt this language in its opinion and never relied on this supposed understanding. The fact that it instead looked to the express statutory exception is a telling rejection of this supposed presumption.

---

172. Another commentator similarly described the lack of a consensus: "Whether such [telegram confidentiality] statutes also prevented government investigators from demanding the production of telegrams was much debated." *The Right to Privacy*, *supra* note 156, at 1901. In 1876 and 1877, while investigating the disputes of the 1876 presidential election, members of Congress extensively debated the extent to which telegrams were privileged. *See id.* at 1902 n.74.

173. 72 Mo. 83 (1880).

174. *Id.* at 90.

175. *Id.* at 92–93.

176. *Id.*

177. *Ex. Parte Brown*, 7 Mo.App. at 492.

The Missouri Supreme Court also explained that telegrams were not "privileged" communications.[178] Wexler argues that this language was about the Missouri statute; the court was construing the statute to not create a privilege because of the public policy in favor of evidence.[179] This appears to be incorrect. The court's discussion of "privilege" occurred before it ever got to its analysis of the Missouri statute. Rather, it was rejecting Chief Justice Cooley's argument that telegrams should be considered privileged *sui generis* like the mail. The court relied on the distinction that telegraphic lines were "not operated by the government," while "the entire postal system is under the control and management of the government."[180]

Similarly, the Northern District of California, in a case interpreting California's disclosure ban, noted the law "provides specifically that they may be disclosed by the lawful order of a court."[181] So, the grand jury subpoena for telegrams was permissible under California law.

The presence of these exceptions for court process suggests that even then, lawmakers considered the disclosure bans to cover compulsory process and did not expect that courts would imply such exceptions; that is why they explicitly exempted court process from the bans. Lawmakers knew how to create broad exceptions for legal process when they wanted to.

Courts today have acted consistent with cases like *Ex Parte Brown*. In *Laxalt v. McClatchy*,[182] for example, the D.C. Circuit held that the Privacy Act did not prohibit disclosure of protected material in discovery because "the plain language of the statute permits disclosure 'pursuant to the order of a court of competent jurisdiction.'"[183] The

178. *Ex Parte Brown*, 72 Mo. at 90–91.

179. Wexler, *supra* note 2, at 2742–43.

180. *Ex Parte Brown*, 72 Mo. at 91.

181. *In re Storror*, 63 F. at 566. *See also* CAL. PENAL CODE § 619 (1880). The court in *In re Storror* used a lengthy quote from a treatise by John Ordronaux. In that treatise, Ordronaux, in summarizing what he believed to be the current state of the law, suggested "even where the statutory prohibition is unqualified, there is always an exception implied in favor of legal process, since obedience to a subpoena is obligatory upon all." ORDRONAUX, *supra* note 160, at 249. He cited no support for this proposition. The Missouri appeals court in *Ex Parte Brown* also made a similar statement but the Missouri Supreme Court did not use this language upon review.

182. 809 F.2d 885 (D.C. Cir. 1987).

183. *Id*. at 888 (quoting 5 U.S.C. § 552a(b)(11)). The *Laxalt* opinion contained statements that, at first blush, could be read as supporting Professor Wexler's argument, such as: "general statutory bans on publication do not bar limited disclosure in judicial proceedings" and "'where Congress has thought it necessary to protect against court use of records it has expressly so provided by specific language.'" *Id*. at 889 (quoting Freeman v. Seligson, 405 F.2d 1326, 1351 (D.C. Cir. 1968)). But, as the D.C. Circuit

courts interpreting the SCA have not acted in a contrary manner; the SCA does not contain a broad exception for all court orders.

Unlike the states just discussed that had specific exceptions for court-based disclosures, Pennsylvania and New Jersey had bans that broadly prohibited the disclosure of "the contents of any dispatch."[184] A separate section made it illegal for a service provider to "unlawfully expose" the contents of a telegram.[185] In a suit between a creditor and debtor, the Pennsylvania Court of Common Pleas (the trial court), interpreting the Pennsylvania disclosure ban, concluded the law allowed disclosures pursuant to legal process because, by definition, these disclosures would not be "unlawful."[186]

Again, modern courts similarly have held that statutes that ban disclosures "unless otherwise provided by law" do not prohibit legal process compelling disclosure.[187] And the courts interpreting the SCA have not acted in a contrary manner; the SCA does not ban only "unlawful" disclosures. It broadly bans all knowing disclosures.

In the nineteenth century, eleven states had statutes prohibiting the "willful" disclosure of communications.[188] Courts interpreted such provisions not to bar disclosures pursuant to legal process because compelled disclosures were not "willful."[189] For example, the Supreme Court of Iowa, in a breach of contract suit, held that the state's statute did not prohibit disclosures pursuant to legal process because

---

later explained, to read these decisions in the way Professor Wexler suggests would be to "seriously overread those precedents." *In re* England, 375 F.3d at 1179. *Freeman*, for example, concerned bans on *publication*, which is distinct from a ban on discovery. *See id.* at 1180.

184. Act of the 14th April, 1851, P.L. 614, sec. 7.

185. Act of the 14th April, 1851, P.L. 614, sec. 8.

186. Henisler v. Freedman, 2 Pars. Eq. Cas. 274, 277 (Pa. Ct. Com. Pl. 1851). *Henisler* conflated the disclosure ban with the separate criminal penalty provision. The ban itself was incredibly broad and prohibited "any person" from taking action that would "make known or cause to be make known, the contents of any despatch." Act of the 14th April, 1851, P.L. 614, sec. 7. It even explicitly made telegrams "inviolable" like the postal mail. The separate criminal penalty provision imposed jail and/or fine for an operator to "unlawfully expose another's business or secrets." The criminal penalty provision, though, did not define the scope of the ban; it only identified the subset of violations that would result in a criminal penalty. The court's decision, then, is circular. It never answered the initial question: is a subpoena compelling disclosure of telegrams lawful under Pennsylvania law? This question can only be answered by looking at the disclosure ban itself. The court instead assumed the subpoena was lawful, which was the question it was supposed to be answering, and then concluded the criminal penalty did not reach a lawful subpoena.

187. *See, e.g.*, *In re* Grand Jury Investigation, No. 17-2587, 2017 WL 11140345, at *3-4 (D.D.C. Oct. 23, 2017), and cases cited therein.

188. Hitchcock, *supra* note 157, at 495. One state, Iowa, used "intentional," which was treated as akin to willful. *Id*.

189. *Woods*, 7 N.W. at 484–85; *Ex parte Brown*, 72 Mo. at 93.

"the person who produces them in obedience to the order is not guilty of voluntarily disclosing their contents."[190] The court continued, "The statute, therefore, does not reach such a case, and is wholly inapplicable." The court never mentioned privileges or the need to strictly construe these statutes or the fact that the statute did or did not specifically mention legal process. Rather, the court looked at the text of the statute and concluded compelled disclosures did not fall within the plain text of the statute.

The SCA does not have a "willful" *mens rea*; it requires a "knowing" *mens rea*. A disclosure pursuant to legal process is a "knowing" disclosure even if not a willful one. The use of a "knowing" *mens rea* suggests that the SCA's disclosure ban does reach compelled disclosures. Otherwise, Congress could have limited the ban to willful disclosures. Overall, these telegraph-era cases support finding that the SCA's broad disclosure ban covers compelled disclosure. The SCA does not contain the limitations that the telegram confidentiality statutes did.

Finally, in the nineteenth century, five states, including Louisiana, had broader disclosure bans without the exceptions identified above but there do not appear to be any reported cases interpreting them. However, the Louisiana disclosure ban was discussed in a report issued by the Judiciary Committee of the U.S. House of Representatives.[191] The House had issued a subpoena for telegrams and the operator refused, citing, in part, the criminal penalty created by Louisiana's disclosure ban.[192] The report explained that a crime required a "willful" *mens rea* and compelled production was not "willful."[193] Thus, the Committee relied not on any presumptions about privileges but on rules governing criminal laws. The SCA does not have a criminal liability provision. In 1918, Louisiana amended its law

190. *Woods*, 7 N.W. at 484–85. The court also appeared to suggest in dicta that compelled disclosures can never be prohibited because "no person can be punished for an act which is not voluntary." *Id.* But there is no dispute that a legislature can ban compelled disclosures, and Professor Wexler's argument is that Congress must be more explicit in doing so. The Supreme Court in *Baldridge*, for example, upheld a broad ban on compelled disclosures. The *Woods* court appears to have been making a statement about criminal liability and not statutory privileges—that no criminal liability can be imposed for involuntary acts. *See* IOWA CODE §10.6 (1873) (noting a violation constituted a misdemeanor). See *infra* for a further discussion of this issue in the context of the Louisiana ban.

191. *See* 44 CONG. REC. 602-04 (Jan. 12, 1877).

192. The Louisiana law at the time stated, in relevant part, "Any operator [or other employee] who shall reveal, make use of or make public any dispatch or message, shall, on conviction, be fined." LA. REV. STAT. § 921 (1870).

193. 44 CONG. REC. 602-04 (House, Jan. 12, 1877). The report also noted that state law could not circumscribe the U.S. House's investigative powers.

to specify exemptions, including allowing disclosures "under due process of any Court of Record. . ." The statute was amended to add a specific exemption to *allow* compelled disclosures.[194] The addition of this exception after the fact is an even stronger indication that there was no well-established default in favor of an implied compulsory process exception. Legislatures felt it necessary to undertake the amendment process to clarify that the disclosure ban did not reach compelled disclosures.

Overall, there does not appear to be a single case from the telegram era that adopted Wexler's argument that legislatures must explicitly mention legal process or discovery in their disclosure bans. No case even relied on a presumption against privilege. Instead, these courts applied the text of the applicable statutes, which, unlike the SCA, did not cover compelled disclosures. The courts interpreting the SCA have reached a different outcome because the SCA is different from the telegram confidentiality statutes in that it has a broader disclosure ban: it covers all "knowing" disclosures instead of only willful or unlawful ones, and it does not contain a catch-all exception for legal process.

D. Federal Communications Act of 1934

The Federal Communications Act of 1934 contained a disclosure ban that is analogous to the SCA's. Section 605(a) contained a ban on service providers disclosing communications transmitted by telegraph, telephone, or radio. In relevant part, the 1934 ban stated, "No person receiving or assisting in receiving, or transmitting, or assisting in transmitting . . . communication by wire or radio shall divulge or publish the existence, contents [etc.] thereof."[195] Congress included several exceptions that were necessary to the operation of the service, such as allowing the communication to be divulged to employees of the service provider and to the addressee, and something as fundamental as a recipient on a ship being able to pass the communication on to the master of the ship. Like with the SCA, the inclusion of these basic, necessary exceptions illustrated the ban's breadth. The list of exceptions also included one for compelled disclosures: "in response to a subpoena [sic] issued by a court of competent jurisdiction, or on de-

194. California similarly amended its disclosure ban in 1880 to add a specific exemption for disclosures pursuant to "the lawful order of a court." *See* 1862 Cal. Stat. 288. Pennsylvania similarly amended its disclosure ban to add a specific exemption for evidentiary disclosure in certain circumstances. 1855 Pa. Laws 530.

195. Pub. L. No. 73-416, § 605(a), 48 Stat. 1064, 1103 (codified at 47 U.S.C. § 605(a)).

mand of other lawful authority." Again, Congress knew how to broadly exempt compelled disclosures when it wanted to; it simply said so. Section 605(a)'s disclosure ban separately prohibited a person who intercepted a communication (as opposed to a service provider) from divulging or publishing its contents to any person. This provision, though, did not contain an explicit exception for legal process. So, section 605(a), like the SCA, specifically included an explicit exception for legal process for certain categories of communications and not others.

In *Nardone v. United States*,[196] the Supreme Court considered whether telephone communications intercepted by federal agents could be admitted into evidence at a criminal trial. Like the SCA disclosure ban, the clause concerning intercepted communications contained no explicit exception for court process. Applying the plain meaning of the statute, the Court held that the intercepted communications could not be admitted into evidence.[197] The language was "clear": "*no person*," which on its face included federal agents, could divulge or publish message contents to "any person."[198] "To recite the contents of the message in testimony before a court is to divulge the message."[199]

Like *Baldridge*, *Nardone* is a significant barrier to Wexler's arguments in favor of defense subpoenas. The Court imposed an evidentiary privilege and excluded otherwise crucial evidence. It did so despite the lack of any explicit clause banning legal process or evidence or mentioning privilege.[200] The Court did not require any specific words. The Court applied the plain text of a broad ban to a situation that was clearly covered (and, that time, to the detriment of the government). *Nardone* also appears to reject Wexler's argument that there is only a "narrow" path to implying a privilege in a disclosure ban, and that path requires a statute that contains no excep-

196. Nardone v. United States, 302 U.S. 379 (1937).

197. *Id*. at 382; *see also* Sablowsky v. United States, 101 F.2d 183, 190–91 (3d Cir. 1938) (finding that intercepted communications could not be admitted into evidence at a criminal trial under section 605(a)'s ban); United States v. Bonanzi, 94 F.2d 570, 571–72 (2d Cir. 1938) (same).

198. *Nardone*, 302 U.S. at 382 (emphasis added).

199. *Id.* at 382.

200. One might argue that this case was decided before the Supreme Court announced the strict construction rule in *St. Regis*. But the Supreme Court was acting under a similar principle in *Nardone*: "Any claim for the exclusion of evidence logically relevant in criminal prosecutions is heavily handicapped. It must be justified by an over-riding public policy expressed in the Constitution or the law of the land." *Nardon*e, 308 U.S. at 340. This principle could not override the plain text of the law. *Id.*

tions.[201] The Communications Act had several exceptions similar to the SCA's, yet those exceptions did not stand in the way of enforcing the plain text of the ban.

Nardone is further proof that courts for the past century have applied the plain text of broad bans to enforce privileges and have not required any specific phrases or "narrow" paths.

IV.
Congress, Not Courts, Should Expand Disclosures under the SCA

When the SCA was enacted in 1986, private information resided primarily on paper. There was no social media, and the Internet and e-mail were in their infancy. The first commercial e-mail client was released in 1988, and Hotmail did not exist until 1996.[202] The Court was dealing with the Fourth Amendment implications of searching stolen stereo equipment.[203] Much has changed. As of 2019, Gmail had 1.9 billion active users, and Internet users send and receive almost 300 billion emails every day.[204] The magnitude of the privacy interests at stake are apparent.

And then there is social media. In December 2020, 2.6 billion people—about one-third of the world's population—were active *daily* on at least one Facebook product (Facebook, Facebook Messenger, WhatsApp, Instagram).[205] These users share 17 billion photos just on Facebook Messenger every month.[206] Snapchat has 383 million users active daily who create and send over 5 billion snaps every day.[207] Stored communications represent a large portion of the private communications of many of the people on this planet. These communications can cover the most intimate aspects of users' lives: discussions about visits to abortion providers, marital issues, drug addiction, being victimized, protests against the government, possibly unethical or illegal conduct, and everything in between.

---

201. Wexler, *supra* note 2, at 2771–73.

202. Sarah Left, *Email Timeline*, The Guardian (Mar. 13, 2022), https://www.theguardian.com/technology/2002/mar/13/internetnews [https://perma.cc/E9DH-SU2E].

203. *See* Arizona v. Hicks, 480 U.S. 321 (1987).

204. *The Shocking Truth About How Many Emails Are Sent*, Campaign Monitor (May 21, 2019), https://www.campaignmonitor.com/blog/email-marketing/2019/05/shocking-truth-about-how-many-emails-sent/ [https://perma.cc/9QPV-W9TS].

205. Facebook, *supra* note 8, at 52.

206. Hutchinson, *supra* note 9.

207. Snap, Inc., Quarterly Report (Form 10-Q), at 24 (April 27, 2023); Snap, Inc., *Q4 Investor Deck* (Feb. 2021), https://s25.q4cdn.com/442043304/files/doc_presentations/presentation/2021/Snap-Inc.-Q4-2020-Investor-Deck.pdf [https://perma.cc/U96E-X8GX]

These technological changes lead to two opposite conclusions. On the one hand, the privacy implications of any disclosure of stored content are immense. If courts were to adopt the recently proposed interpretation of the SCA disclosure ban allowing non-governmental subpoenas, billions of communications would suddenly be subject to new disclosures to new parties in civil and criminal litigation all through local, state, and federal court systems and in administrative proceedings.

But the privacy implications are even broader. Currently, a service provider often produces the entire account record to the government, and not just the relevant portion, at which point the government reviews the entire account and segregates out the relevant information.[208] Because service providers say they do not have the capacity to perform the segregation before production (and defense attorneys may not want them to), the providers may take the same approach with all the newly allowed legal process. The production of the entire account implicates the privacy interests not just of the account holder but also the hundreds or thousands of individuals with whom the holder communicated. And such information plausibly could be sought in every case for every potential government witness or government agent involved in the investigation.

On the other hand, parties increasingly need to be able to obtain this content in litigation. Criminal cases—reflecting the changes in broader society—have changed and now depend more and more on electronic evidence, especially electronic communications undertaken through third-party service providers. These changes have meant that the government's case often relies on electronic communications and any defense is more likely to as well.

Part IV.A explains that the current regime is not as harsh as suggested by Wexler and other recent commentators. In the vast majority of cases, defendants can obtain access to the content information without being blocked by the SCA.

The final Part explains why Congress needs to amend the SCA. Congress has the institutional competency to overhaul the SCA and the necessary tools to do so in an organized manner.

A. The Non-Harshness of the Current System

As most readers are aware, more than ninety percent of federal criminal cases are resolved before trial, usually through a guilty plea.

208. *See* United States v. Aboshady, 951 F.3d 1, 5 (1st Cir. 2020); United States v. Purcell, 967 F.3d 159, 173–75 (2d Cir. 2020).

Third-party discovery is rare in these cases, and the parties typically do not even obtain authority to issue subpoenas pursuant to Federal Rule of Criminal Procedure 17, which is primarily for preparing for trial. Some courts require that Rule 17 subpoenas only seek documents that would be admissible at trial.[209] Thus, in the vast majority of cases, third-party subpoenas to service providers will not be sought.[210]

For the small number of defendants who will proceed to trial, in most instances they will be able to obtain the relevant evidence for the reasons described below. It may be why in the thirty-five years since the SCA was enacted, there have been very few cases, newspaper articles, or commentary about defendants being denied access to material information.[211]

First, recall that the defense already has access to non-content information, including through compulsory process. It can use this information to identify account subscribers and obtain their content from them. Separately, often the non-content information itself will be what is important for the defense. For example, according to Wexler, one recent article cited the case of an Iraqi man facing extradition whose attorneys wanted login data, presumably to show circumstantially that

209. *See, e.g.*, United States v. Louis, No. 04-203, 2005 WL 180885, at *3 (S.D.N.Y. Jan. 27, 2005) (explaining the purpose of 17(c) subpoena is "trial-focused" and may be used "only to obtain materials admissible as evidence at trial"); United States v. Smith, No. 19-cr-00669, 2020 WL 4934990, at *2–4 (N.D. Ill. Aug. 23, 2020) (discussing cases).

210. It appears unlikely that so many cases end in a plea because defendants lack access to user content. As explained in this section, defendants likely have access to user content in most circumstances if needed. Also, as a general matter, the government bears the burden of proving its case. Defendants do not need to produce any evidence to win their case. Lastly, if evidence would tend to prove innocence, defense attorneys are unlikely to forego the effort at least to seek that evidence.

211. Wexler speculates there may be a broad "chilling effect" such that criminal defense attorneys do not even try to obtain content in light of the disclosure ban. Wexler, *supra* note 2, at 2740. Professor Wexler admits it is impossible to know the extent of this phenomenon but attempts to quantify it by noting that "U.S. law enforcement served Facebook with legal demands for data from 82,321 accounts" (and similarly for other large tech companies) and comparing that to the number of federal cases. *Id*. at 2728. But the statistics cover local, state, and federal law enforcement, not just federal. They also cover civil and administrative government proceedings, not just criminal cases. It is impossible to make any sort of a useful comparison. And, importantly, the statistics cover data requests for content and non-content information, and the latter already are available to the defense. In fact, defense attorneys do not appear to issue legal process for non-content information in substantial numbers even though they are allowed to and even though this would be a first step to obtaining content information. In any case, defense attorneys likely would issue a subpoena (to the service provider directly or to a user) for information that is material and potentially exculpatory, at least to preserve the issue for appeal and protect themselves from charges of ineffective assistance.

he was not at the location of the murder.[212] Account login data, such as date, time, and IP addresses of logins, are *already* available to the defense through subpoenas.

Second, the government is likely to obtain the relevant electronic evidence and turn it over in discovery. The government decides the case to build and which events or individuals to focus on.[213] The government will obtain the evidence relevant to these events or individuals to investigate the possibility of criminal charges and to build its case. It will disclose the relevant evidence, whether helpful or unhelpful, to the defense.

Theoretically, the government may try to avoid obtaining information that is helpful only to the defense. But in its preliminary investigation, the government may not know precisely which accounts contain incriminating information and therefore will need to obtain information from any relevant accounts. The same account may contain both incriminating and exculpatory information. In the context of electronic evidence, this approach is even more comprehensive. Suppose the government identifies the Facebook account of witness A as containing incriminating evidence. Upon issuance of a search warrant, Facebook will produce the entirety of witness A's account data, not just the relevant information. The government must review the information and turn over not just the incriminating information but also exculpatory or potentially exculpatory information in the account data. In this way, the government will end up in possession of potentially exculpatory information to be turned over to the defense.

And even if the government does know which accounts contain incriminating information, it is not always in the government's interest to skip accounts with possibly exculpatory information. The defense, even if it cannot use compulsory process, can use other exceptions to obtain content, such as issuing a subpoena to the sender or recipient or obtaining their consent to have the service provider disclose communications. If the government avoids obtaining relevant information, it

212. Wexler, *supra* note 2, at 2723.

213. As two notable commentators explained, "In most cases in which Internet communications are a key piece of evidence, law enforcement has used the investigative tools (search warrants, court orders, and grand jury subpoenas) specified by the SCA to compel the lawful production of such information in the process of building its case. . . . In a standard case, then, a defendant may rely on the government to turn over, from the set of Internet communications the government deemed significant enough to compel, at least those communications upon which the government intends to rely or that favor the defendant." Marc. J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 592 (2007).

risks the defense later obtaining this information through one of the other exceptions and using it to attack the government's case. The government will prefer to know the nature of relevant information before bringing charges.

Third, in many instances, the evidence will only be relevant if the defendant received or sent the communication. For example, this evidence could help disprove the defendant's state of mind or the requisite *mens rea* for the offense, such as a lack of intent to defraud or lack of knowledge. For the messages the defendant sent or received, the government will be able to obtain the communications through either the sender/recipient or consent exceptions. Take, for example, Wexler's example of a defendant on trial for murder who wanted to present evidence that he received threatening messages from the victim on Instagram.[214] Although the article does not contain many details, there appear to be four possibilities. The victim had sent threatening messages directly to the defendant, in which case he could retrieve them through the consent or recipient exceptions. Or the victim publicly posted the messages. At least one case has held that social media companies must produce them under the theory that the user implicitly consented to their production by making the messages public.[215] Third, the messages could be obtained directly from the victim. Lastly, if the information was deleted, it likely was no longer available regardless of legal process (and recall the defense does not have the ability to require service providers to preserve data).[216]

Wexler criticizes these alternative methods, such as consent or subpoenaing the sender/recipient, because they result in notification to the account user, which can lead to evidence destruction, flight, or other negative consequences.[217] But service providers disclose subpoenas to users unless the subpoena is accompanied by a court order barring disclosure.[218] The basis for a non-disclosure order is section

214. Wexler, *supra* note 2, at 2738.

215. Facebook, Inc. v. Superior Court, 417 P.3d 725 (Cal. 2018).

216. *See, e.g.*, *Help Center: What Happens to Content (Posts, Pictures) That I Delete From Facebook*, FACEBOOK, https://www.facebook.com/help/121995105053180?helpref=related&ref=related&source_cms_id=356107851084108&rdrhc [https://perma.cc/XJL9-LHP4] (last visited Apr. 4, 2023) (noting when content is deleted, it is "it is permanently deleted from your Facebook account . . . [and] from our servers and backup systems, so we're unable to retrieve this deleted content."). And, section 2703(f)'s information preservation process is unavailable to the defense without statutory amendments.

217. Wexler, *supra* note 2, at 2741.

218. *See, e.g.*, *Google Help: Serving Civil Subpoenas or Other Civil Requests on Google*, GOOGLE, https://support.google.com/faqs/answer/6151275?hl=EN [https://perma.cc/4WW2-HYCA] (last visited Apr. 4, 2023); APPLE, LEGAL PROCESS GUIDE-

2705, which allows the government to seek delaying notification to the user if there are concerns about flight, destruction of evidence, and so on. Under the provision's plain language, it is unavailable to the defense (likely worded this way because Congress did not allow for non-governmental content subpoenas). Implying defense subpoenas into the SCA still will not allow the defense to avoid user notification. Authority to issue non-disclosure orders comes from statutes.[219] Federal courts do not have plenary authority to issue non-disclosure orders under Rule 17.[220]

Fourth, another large category of electronic communications is for impeachment of government witnesses and government agents. For government agents, the subpoena can be served on the government to obtain and produce impeachment information consisting of electronic communications. As for government witnesses, by definition, this evidence is relevant only if the government plans to call the witness at trial. In that case, the defense will be able to serve a subpoena with the aid of the government or, if the government refuses, directly on the witness after obtaining the witness's location from the government. The witness then can retrieve the account information and provide it for the defendant's review.[221]

Lastly, communications involving individuals who will not be witnesses and which the defendant did not receive or send will rarely be relevant or admissible. For the government, this information can be valuable because it may be admissible under a co-conspirator hearsay exception.[222] For the defense, in many circumstances these statements will be inadmissible. Recall that many courts do not allow Rule 17 subpoenas for inadmissible information. Maybe the information could lead to admissible evidence, such as if one of the participants is called as a witness and the communications are used to impeach. But it is

---

LINES: GOVERNMENT & LAW ENFORCEMENT WITHIN THE UNITED STATES, https://www.apple.com/privacy/government-information-requests/ [https://perma.cc/7GXS-CGUU] (last visited Apr. 4, 2023) ("Apple will notify customers when their Apple account information is being sought in response to legal process from government, law enforcement, or third parties. . .").

219. *See, e.g.*, 12 U.S.C. §§ 3409, 3420(b); 18 U.S.C. §§ 1510(b), § 2705.

220. *See, e.g.*, In re Appl. of the U.S. for an Ord. Pursuant to 28 U.S.C. § 1651(A), No. 17-mc-01604 (BAH), 2017 WL 3278929 (D.D.C. July 7, 2017) (noting in rare circumstances courts can issue non-disclosure orders for a Fed. R. Crim. P. 17 grand jury subpoena pursuant to a court's exercise of its residual authority as authorized by the All Writs Act, 28 U.S.C. § 1651).

221. Joshua A. T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1055–65 (2014). Professor Wexler cites a case in which social media companies refused to disclose to the defense content from the accounts of prosecution witnesses but it is unclear if the defense subpoenaed the witness. Wexler, *supra* note 2, at 2723.

222. *See* FED. R. EVID. 802(d)(2).

unclear if Rule 17 subpoenas can be used for such information, and in any case, the subpoena can be issued to the witness, as described above. The primary instance where such communications may be relevant is as impeachment information for witnesses the defense may call. This information would be important to have to control the witness during testimony and impeach if the witness testifies in a manner inconsistent with the electronic communications. But, in this instance, the witness is available to the defense and would receive a subpoena for their electronic communications—similar to impeachment information for the government's witness.

There will be instances where these avenues are unavailable and the defense's only option would be to compel production from the service provider. For example, state law may prohibit defendants from obtaining information from a victim. Or a user may be deceased and, if the account has not been deleted, the defense may need to obtain the account content. Although the user could never be a witness, the account's content may lead the defense to other relevant witnesses or may contain exculpatory information that the defense could show the government. Even this is not a complete roadblock as at least one court has held that the personal representative of the decedent's estate can provide consent to require disclosure of account content.[223] Similarly, even if the user is alive, it may be impossible to locate the user to obtain consent. But these represent a very small subset of possibilities and the likelihood that the content contains material, exculpatory, admissible evidence is even lower.

One criticism might be that if defendants already have access to necessary electronic evidence in most instances, then the privacy implication of fully allowing defense subpoenas for user content is actually insignificant. Several privacy concerns remain, though.

First, there is a substantial difference between obtaining user content from the user or pursuant to the user's consent, as opposed to bypassing the user and obtaining it directly from the service provider. In the former circumstance, the user has the opportunity and incentive to object to the subpoena or to its breadth. The user can seek to narrow or quash the subpoena and protect their privacy. But the user content does not represent the privacy of the service provider. Therefore, the service provider is unlikely to have the incentive or ability to challenge the subpoena. The service provider does not know what is particularly private in the account and is unlikely to be responsive to litigation in which it is uninvolved. It is unlikely to expend significant

223. *See* Ajemian v. Yahoo!, Inc., 84 N.E.3d 766, 773–74 (Mass. 2017).

resources to undertake these tasks to challenge each subpoena. Importantly, the user can also produce only the items directly responsive to the subpoena, thus minimizing the privacy invasion. As noted above, service providers often produce the contents of the entire account, thereby maximizing the privacy intrusion. Defense attorneys, defendants, and others would likely have access to the entire account contents. Going directly to the service provider would represent a significant expansion of the privacy invasion.

Second, the privacy implications are significant because privacy is not just about access to content but the possibility of access to content. For example, even today, the government seizes a miniscule fraction of all electronic communications. Yet, service providers and the public have expressed alarm at the government's ability to access all this information. Users may perceive their privacy is being invaded further by the possibility that many additional litigants could access their accounts. These concerns may speed the development and implementation of additional blocking technologies like encryption, which would only further denigrate the search for truth. These are complex, multi-faceted issues—for Congress to address.

B. The Preference for Congress to Act

As described above, this Article acknowledges that there could be rare instances in which a defendant must obtain user content but is unable to do so without going to the service provider. It is better for Congress to weigh the need to resolve these rare instances with the resulting impact to privacy described above. Turning to Congress instead of the courts to amend the SCA is consonant with the respective roles of courts and legislatures. Congress can balance the various privacy and liberty interests at stake.

Another benefit of going through Congress is that a statutory amendment would allow Congress to make the entirety of the SCA consistent with an exception for defense subpoenas for content. Congress could prescribe the specific requirements that must be satisfied before a court can issue a defense subpoena for content to best balance the needs of defendants with the protection of privacy.[224] For example, Congress might first require defendants to seek consent or obtain the data from the sender or recipient. Congress might require defendants to apply for a court order for each account. When the govern-

224. *See, e.g.*, Brendan Sasso, *Digital Due Process: The Government's Unfair Advantage Under the Stored Communications Act*, 8 VA. J. CRIM. L. 35, 36–37, 57 (2020) (proposing a standard Congress could enact for courts to apply).

ment compels disclosure, it must first obtain a search warrant, which is the most onerous legal process available within our legal system and involves close judicial oversight. But, of course, criminal defendants cannot apply for search warrants.

Currently, some courts are not at all involved in the issuance of document subpoenas; others grant a blanket request for both parties to issue pretrial subpoenas, allowing either party to issue subpoenas without court oversight.[225] The lack of consistent court oversight presents a significant privacy concern with the tens of thousands of ongoing civil, criminal, and administrative proceedings in the United States. Requiring a court order would inject additional court oversight that could ameliorate privacy concerns.

Congress might also require a higher standard to obtain a subpoena for content, such as more specific and direct proof that the information will be material to a defense or something akin to a search warrant's probable cause requirement. On the other hand, if Congress enacts other privacy protections, it might ease subpoena requirements; some courts, for example, currently only allow subpoenas for admissible information. Congress therefore could allow defendants more freedom to conduct investigations.

Similarly, Congress can create procedures to deal with the privacy implications of service providers producing entire account records pursuant to a subpoena instead of only the relevant information. For example, it could make the entire account accessible only to defense counsel, who can segregate the relevant information and share it with their client, which would lessen the privacy implications for the mass of irrelevant communications contained in the account record.

Statutory amendments also could give the defendants tools to deal with the new challenges presented by electronic evidence. For example, Congress can decide under what circumstances defendants can require a service provider to preserve information while they obtain the necessary legal process. The defense may need this authority as disappearing messages have become more popular and service providers implement auto-deletion policies. But Congress will need to balance a variety of different interests at stake: service providers' de-

225. *See, e.g.*, United States v. Llanez-Garcia, 735 F.3d 483, 498–99 (6th Cir. 2013) (identifying district courts that require court involvement and others that do not); United States v. Urlacher, 136 F.R.D. 550, 554–555 (W.D.N.Y. 1991) (same); United States v. Cartagena-Albaladejo, 299 F. Supp 378 (D.P.R. 2018) (noting the District of Puerto Rico contains no requirement for prior judicial approval for subpoenas); Khouj v. Darui, 248 F.R.D. 729, 730 (D.D.C. 2008) (granting broad authority to a criminal defendant to issue subpoenas).

sire to follow through on their promises to users to maintain privacy by deleting communications; service providers' continued ability to market these features; users' expectations that their communications will be deleted and not preserved; the defense's need to preserve possibly valuable information; and the service providers' need not to overburden staff and systems with a large number of preservation requests.

Also, Congress can dictate under what circumstances service providers can be prohibited from disclosing to the subscriber a defense's subpoena so as to protect the information from being destroyed, prevent flight of relevant witnesses, and preserve the defense's ability to continue its ongoing investigation. These provisions are available to the government currently but can only be made available to the defense through statutory amendments. Given the ease with which information can be destroyed, these provisions could be important for the defense.

There are many other policy decisions Congress will need to make regarding defense subpoenas. Congress will decide whether to require reimbursement for defense subpoenas and the standard for reimbursement courts will apply for indigent defendants. Congress may decide to extend section 2703's immunity provision to defense subpoenas. Or it may not if defense subpoenas require more court oversight anyway. Allowing suits against service providers for defense subpoenas would be more protective of privacy. And Congress will decide whether to create penalties for defense counsel who re-disclose content improperly, as it has done for government attorneys. Doing so would be more protective of privacy but may raise unique constitutional or other concerns about rights to counsel and access to evidence. Defense subpoenas for content cannot be simply wished into existence by courts; many fundamental policy decisions must be made to balance a variety of important but competing interests among defendants, service providers, and users.

It is unclear when and how Congress will act to update the SCA to reflect the revolutionary technological changes that have taken place since 1986.[226] Today, there is broad agreement to update the SCA and increasing clamor to do so.[227] If the law is updated, it may provide an opening to include some provision for defense compulsory process.

---

226. *See* Sasso, supra note 224, at 37 (noting the House of Representatives passed legislation updating the SCA in 2016 and 2017 but the efforts died in the Senate).
227. *See, e.g.*, *id.* (noting "broad support" for updating the SCA).

CONCLUSION

Our legal system seeks truth but not at all costs. It is not unusual for the value of privacy or privileges to outweigh their cost to the truth. Privileges are scattered throughout the federal code and in the laws of all fifty states. The right to privacy enshrined in the Fourth Amendment impedes the government's plans. Striking the right balance between the value of privacy or a privilege on the one hand and its cost to the truth on the other requires difficult policy judgments. Congress struck a balance in the SCA. Through the SCA, Congress has protected the privacy of the most intimate communications of billions of people around the world. It did so through a broad and comprehensive disclosure ban. This ban covers all knowing disclosures by the online company, including those sought pursuant to subpoenas not issued by the government. The SCA is highly protective of privacy, in part because of the troubling circumstance that a third-party company holds these private and intimate communications. These companies may not have the same incentive to protect privacy as the users whose privacy is actually at stake.

Society also has a strong incentive to give criminal defendants the tools to defend themselves when their liberty is at stake. This Article shows that in all but the rare circumstances, the SCA does not block access to those tools for criminal defendants. If Americans today believe Congress originally struck the wrong balance with the SCA's disclosure ban, it will need to be Congress that re-weighs the different interests at stake and strike a different balance. It will need to be Congress that harmonizes any changes to the scope of the disclosure ban with the rest of the intricate statute. Until then, courts cannot unilaterally amend the disclosure ban, as Professor Wexler's argument requires. Doing so would not only be contrary to the function of courts but would create a statutory mess and require even further judicial legislating to make sense of the resulting mess.