# PRIVACY AS PRIVILEGE: THE STORED COMMUNICATIONS ACT AND INTERNET EVIDENCE

*Rebecca Wexler*

## CONTENTS

INTRODUCTION ..... 2723
I. THE INTERNET AND THE TELEGRAPH ..... 2730
*A. The Puzzle* ..... 2731
*B. The Stored Communications Act* ..... 2735
*C. Telegraph Privacy Statutes* ..... 2741
II. PRIVACY AS PRIVILEGE ..... 2745
*A. Statutory Privileges* ..... 2745
*1. Defining Statutory Privileges* ..... 2745
*2. Common Features of Privileges* ..... 2748
*3. Confidentiality Without Privilege* ..... 2750
*4. The Current Stored Communications Act Privilege* ..... 2753
*B. The Rules that Govern Statutory Privilege Construction* ..... 2757
*1. The Strict Construction Rule* ..... 2757
*2. Express Statutory Privileges* ..... 2762
*3. Implied Statutory Privileges* ..... 2767
*4. Misconstruing the Stored Communications Act* ..... 2773
III. THE POLICY OF AN INTERNET COMMUNICATIONS PRIVILEGE ..... 2778
*A. Correcting the Current Case Law* ..... 2779
*1. Privacy Interests* ..... 2779
*2. Service Provider Interests* ..... 2782
*B. Considering a Novel "Medium" Privilege for the Internet* ..... 2785
*1. Privacy and Privilege Law's Shared Theoretical Concerns* ..... 2786
*2. Applying Privilege Analysis to the Internet* ..... 2788
CONCLUSION ..... 2792

# PRIVACY AS PRIVILEGE: THE STORED COMMUNICATIONS ACT AND INTERNET EVIDENCE

*Rebecca Wexler*[*]

*This Article exposes a profound and growing injustice that major technology companies have propagated through every level of the judiciary under the guise of protecting data privacy. The Supreme Court has repeatedly proclaimed: "In our judicial system, the public has a right to every [person's] evidence." Yet, for over a decade, Facebook, GitHub, Google, Instagram, Microsoft, and Twitter have leveraged the Stored Communications Act (SCA) — a key data privacy law for the internet — to bar criminal defendants from subpoenaing the contents of another's online communications, even when those communications could exonerate the wrongfully accused. Every appellate court to rule on this issue to date has agreed with the companies.*

*This Article argues that all of these decisions are wrong as a matter of binding Supreme Court doctrine and just policy. The Article makes two novel doctrinal claims and then evaluates the policy consequences of those claims. First, when courts read the SCA to block criminal defense subpoenas, they construe the statute as creating an evidentiary privilege. Second, this construction violates a binding rule of privilege law: courts must not construe ambiguous silence in statutory text as impliedly creating a privilege because privileges are "in derogation of the search for truth." This Article is the first to read the SCA through the lens of evidentiary privilege law. Overturning the conventional wisdom and correcting the erroneous case law on this issue will enhance truth-seeking and fairness in the criminal justice system with minimal cost to privacy.*

---

[*] Assistant Professor, University of California, Berkeley School of Law. This Article received the 2020 Privacy Law Scholars Conference Reidenberg-Kerr Award for "overall excellence of a paper submitted by a pre-tenure scholar."

This Article benefited from workshops at Berkeley School of Law, Fordham University School of Law, The Ohio State University Moritz College of Law, UCLA School of Law, University of California, Irvine School of Law, University of Chicago Law School, Stanford Law School, Yale Law School, the Center for Advanced Study in the Behavioral Sciences at Stanford University, the Privacy Law Scholars Conference, the Privacy Law Forum, the Internet Law Works-in-Progress Conference, and the Evidence Summer Workshop. For detailed comments on prior drafts, the author thanks Dan Burk, Simon Cole, Vikas Didwania, Mark Gergen, Aziz Huq, Edward Imwinkelried, Orin Kerr, Paul Ohm, Andrea Peterson, Andrea Roth, Pam Samuelson, Paul Schwartz, and Ari Waldman. The author thanks Ron Allen, Jack Balkin, Ken Bamberger, Bicka Barlow, Franziska Boehm, Kiel Brennan-Marquez, Ryan Calo, Linc Caplan, Erwin Chemerinsky, Bryan Choi, Danielle Citron, Julie Cohen, Catherine Crump, Ellen Deason, Jim Dempsey, Deven Desai, Niva Elkin-Koren, Hanni Fakhoury, Peter Galison, Brandon Garrett, Jonah Gelbach, Albert Gidari, Jonathan Gould, Megan Graham, Jerome Greco, Woodrow Hartzog, Chris Hoofnagle, Kirsty Hughes, Pam Karlan, Don Landis, Mark Lemley, Karen Levy, William McGeveran, Priscilla Regan, David Sklansky, Tyler Slay, Chris Soghoian, Jeff Stein, Steven Sugarman, Olivier Sylvain, Kate Tesch, Maggie Wittlin, and Diego Zambrano. This Article benefited immensely from reference support from Doug Avila, Marci Hoffman, Dean Rowan, and I-Wei Wang, and from research assistance from Kristina Chamorro, Robert Fairbanks, Chelsea Hanlock, Joon Hwang, Joseph Kroon, David Murdter, Shreya Santhanam, Cheyenne Smith, Nivedita Soni, Tyler Takemoto, and Daniela Wertheimer. The editors of the *Harvard Law Review* provided invaluable editorial assistance.

## INTRODUCTION

A homicide defendant in California was blocked from arguing self-defense because he was denied access to the records of harassing online messages and death threats that had kept him "in constant fear for his life."[1] A murder defendant in the District of Columbia was denied access to impeachment material from a key prosecution witness's social media accounts, despite the trial judge's finding that the evidence was relevant, material, and necessary to vindicate his "fundamental constitutional rights."[2] A death row inmate in Texas was denied access to the source code for a forensic software program used to analyze the evidence against him, despite a judge's finding that the code was "material and necessary for the administration of justice."[3] An Iraqi refugee, accused of terrorism and facing extradition, torture, and "almost certain death,"[4] was denied access to Facebook and Twitter posts that might have helped exonerate him.[5]

The Supreme Court has repeatedly declared: "In our judicial system, the public has a right to every [person's] evidence."[6] Yet, in each of these cases, and many more like them,[7] technology companies, including

---

[1] Opposition to Non-party Instagram Motion to Quash Subpoena Duces Tecum at 5, People v. [Redacted], No. [Redacted] (Cal. Super. Ct. Nov. 13, 2018) (on file with the Harvard Law School Library) [hereinafter Opp'n to Instagram Motion]; *see also id.* at 1 & n.1, 4–6, 8; *id.* at 14 Exhibit A (subpoena duces tecum to Facebook, Inc. (Instagram)).

[2] Brief for the United States at 3, Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019) (No. 18-SS-958) (on file with the Harvard Law School Library) (describing the trial court's order denying Facebook's motion to quash); *see also Wint*, 199 A.3d. at 628; Brief for the United States, *supra*, at 4.

[3] Order and Certificate, *Ex parte* Colone, No. 10-10213 (Tex. Dist. Ct. Jan. 3, 2020) (on file with the Harvard Law School Library); *see* Protective Order, *Ex parte* Colone, No. 10-10213 (Tex. Dist. Ct. Nov. 21, 2019) (on file with the Harvard Law School Library); Order Denying Petitioner Joseph Colone's Amended Notice of Motion and Motion to Compel Production of Records Pursuant to Cal. Penal Code 1334.2, *In re* Colone, No. 20-517083 (Cal. Super. Ct. July 28, 2020) (on file with the Harvard Law School Library) [hereinafter Order Denying Colone's Motion].

[4] Ben Taub, *The Fight to Save an Innocent Refugee from Almost Certain Death*, NEW YORKER (Jan. 20, 2020), https://www.newyorker.com/magazine/2020/01/27/the-fight-to-save-an-innocent-refugee-from-almost-certain-death [https://perma.cc/53Y7-WVHN].

[5] Audrey McNamara, *Facebook, Twitter Withheld Data that Could Prove Refugee's Innocence in Murder Case, Attorneys Say*, CBS NEWS (Jan. 23, 2020, 11:19 AM), https://www.cbsnews.com/news/omar-ameen-facebook-twitter-withheld-data-that-could-prove-refugees-innocence-in-murder-case-attorneys-say-2020-01-22 [https://perma.cc/J7NN-YUFK] (documenting Facebook's and Twitter's reliance on the Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712, to refuse to comply with a criminal defense subpoena seeking posts from suspended ISIS social media accounts).

[6] For the latest in a long line of cases repeating this maxim, see *Trump v. Vance*, 140 S. Ct. 2412, 2420 (2020) (internal citation and quotation marks omitted).

[7] Petition for a Writ of Certiorari at 11–14, Facebook, Inc. v. Superior Ct., 140 S. Ct. 2761 (2020) (No. 19-1006), 2020 WL 70352 (collecting cases); Memorandum of Law in Support of Non-party Microsoft Corporation's Motion to Quash Defendant Saldarriaga's Subpoena at 6–11, United States v. Mejia-Saldarriaga, No. 11-cr-987 (S.D.N.Y. Dec. 17, 2013).

Facebook, GitHub, Google, Instagram, Microsoft, and Twitter, have argued that the Stored Communications Act[8] (SCA) — a key data privacy law for the internet — gives the companies special entitlements to not comply with judicially ordered compulsory process, and that those entitlements are more important than the life and liberty of the criminally accused. Indeed, Facebook and Twitter recently argued to the Supreme Court that it is wrong to "prioritize[] a criminal defendant's desire to obtain" relevant, exculpatory evidence over "trust in the privacy of electronic communications," because doing so "threatens to discourage the use and development of innovative technologies."[9] To date, the courts have agreed.

For over a decade, federal and state courts across the country have construed the SCA to bar criminal defendants from subpoenaing technology companies for the contents of another's electronic communications.[10] Section 2702(a) of the SCA mandates that electronic communication service providers "shall not knowingly divulge to any person or entity the contents of a communication."[11] Section 2702(b) then lists nine express exceptions for permissible disclosures of communications contents, including disclosures to an intended recipient of the communication, disclosures necessary to the rendition of the service, and disclosures to governmental entities pursuant to certain forms of legal process.[12] The text is silent on criminal defense subpoenas,[13] as is the

---

[8] 18 U.S.C. §§ 2701–2712.

[9] Petition for a Writ of Certiorari, *supra* note 7, at 10.

[10] *See generally* 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 (2007) (describing the issue of a purported SCA block on criminal defense subpoenas).

[11] 18 U.S.C. § 2702(a)(1). Service providers treat the "contents" of a communication to include not merely the bodies of emails and text messages but also documents, photographs, videos, and voice messages. *See United States National Security Requests for User Information,* GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/us-national-security [https://perma.cc/9EY5-CW8E] (listing examples of content). GitHub treats computer source code stored in private repositories as contents for purposes of responding to legal process. *See Guidelines for Legal Requests of User Data*, GITHUB (2021), https://docs.github.com/en/github/site-policy/guidelines-for-legal-requests-of-user-data [https://perma.cc/W3JQ-JSLJ]; *see also* GITHUB, 2019 TRANSPARENCY REPORT (2020), https://github.blog/2020-02-20-2019-transparency-report [https://perma.cc/8ENF-9BWY]. In some circumstances, URLs may constitute communications contents. *See In re* Google Inc. Cookie Placement Consumer Priv. Litig., 806 F.3d 125, 135–39 (3d Cir. 2015); *see also* Joel Reidenberg, Norman I. Silber, Peter Drew Kennedy & Ronald Abramson, *Panel III: The Privacy Debate: To What Extent Should Traditionally "Private" Communications Remain Private on the Internet?*, 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 329, 373–75 (1995) (addressing protections for content versus noncontent information in early drafts of the SCA).

[12] 18 U.S.C. § 2702(b)(1)–(9). The Fourth Amendment likely also requires a warrant. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010).

[13] *See* 18 U.S.C. § 2702(b)(1)–(9).

legislative record.[14] Nonetheless, courts and commentators alike have concluded that the SCA bars disclosures pursuant to such subpoenas without qualification. When communications are unavailable from other sources, such as when subpoenaing an account holder directly would be dangerous or impossible or would risk destruction of evidence, the current SCA case law can completely suppress relevant, exculpatory evidence.

This Article argues that all of these decisions are wrong — as a matter of binding Supreme Court doctrine and just policy. It makes two novel doctrinal claims and then evaluates the policy implications of those claims. *First*, courts have construed the SCA as creating an evidentiary privilege. *Second*, this construction violates a binding rule of privilege law: courts must not construe ambiguous silence in statutory text as impliedly creating a privilege because privileges are "in derogation of the search for truth."[15] While existing legal authorities are admittedly vague in defining what constitutes a privilege, this Article shows that the central function of a privilege is to exempt an ex ante category of information from compulsory process. Construing the SCA as a bar on criminal defense subpoenas does just that. This Article is the first to examine the SCA through the lens of evidentiary privilege law. The cases comprising the current consensus view of the SCA never considered and do not address the arguments presented here.

At first glance, the current consensus view appears to cede judicial control by abrogating the compulsory process powers of the courts, along with those of the litigants before them. But, on closer examination, the view is a stealth overreach in the guise of judicial restraint. Judges perpetuating the consensus reading of the SCA have impermissibly expanded their authority by facilely concluding that Congress dictated the recognition of a novel privilege for the internet through ambiguous silence in the SCA's text, while shirking the careful balancing of competing interests that would be required before courts could create an analogous privilege via their common law authority.[16] Courts are not deferring to Congress when they construe the SCA as creating a privilege; they are subsidizing technology companies by exempting them from the burdens of complying with judicial process that other companies and private persons all must bear. The result obscures the origins

---

[14] Reviewing thousands of pages of legislative history revealed just two witnesses with clarifying questions on nongovernmental subpoenas and one passing mention — in one individual's testimony at a congressional hearing that took place in 1984, two years prior to the enactment of the law — of a subpoena that, based on the fact pattern described, might have been issued by a criminal defendant, though it was not expressly identified as such. *See infra* pp. 2776–78.

[15] United States v. Nixon, 418 U.S. 683, 710 (1974).

[16] *See* Jaffee v. Redmond, 518 U.S. 1, 9–10 (1996); Trammel v. United States, 445 U.S. 40, 50–51 (1980).

of privilege rules and masks responsibility for controversial policy choices.

In many ways, it is unsurprising that an erroneous view of the SCA as barring judicially ordered criminal defense subpoenas has proliferated through the courts. On the one hand, this view has been advanced by multinational companies with power and privilege, backed by Gibson, Dunn & Crutcher,[17] Covington & Burling,[18] Perkins Coie,[19] Mayer Brown,[20] Orrick, Herrington & Sutcliffe,[21] and other major law firms acting as repeat litigators on the issue.[22] On the other hand, this view has been marshaled against underresourced, decentralized public defenders managing full felony dockets and representing poor, disproportionately Black, and marginalized clients. In the words of one federal defender: "Do I think that the content would be really helpful? Yes. Do I think that we could beat Facebook and Twitter in court? Probably not."[23] Meanwhile, experts commenting on this issue in *Wired* magazine,[24] *The New York Times*,[25] *The Washington Post*,[26] the *Los Angeles*

---

[17] *See* Petition for a Writ of Certiorari, *supra* note 7, at 22 (representing Facebook and Twitter).

[18] *See* Order Denying Colone's Motion, *supra* note 3 (representing GitHub).

[19] *See* Petition for a Writ of Certiorari, *supra* note 7, at 22 (representing Facebook and Twitter).

[20] *See* Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 727 (Cal. 2018) (representing Google).

[21] *See* Memorandum of Law in Support of Non-party Microsoft Corporation's Motion to Quash Defendant Saldarriaga's Subpoena, *supra* note 7, at 12 (representing Microsoft).

[22] *Cf.* Ari Ezra Waldman, *Privacy Law's False Promise*, 97 WASH. U. L. REV. 773, 791–824 (2020) (theorizing "legal endogeneity" in privacy law, *id.* at 791, whereby legal institutions defer to corporate symbolic compliance with ambiguous elements of law until, through a process of "managerialization," *id.* at 808, corporate interpretations of law "become embedded in institutional interpretations of law," *id.* at 791). Silence in section 2702 as to defense subpoenas may create ambiguity and thus predictable legal institutional deference, or institutional deference to corporate interpretations of the law. *See* Ryan Calo, *Privacy Law's Indeterminacy*, 20 THEORETICAL INQUIRIES L. 33, 42 (2019) (observing that the need to balance privacy with other values, such as security, "is a systemic source of indeterminacy in privacy law"); Olivier Sylvain, *Recovering Tech's Humanity*, 119 COLUM. L. REV. F. 252, 253 (2019) (arguing that "courts have abjured their constitutional authority to impose legal duties" on tech companies).

[23] McNamara, *supra* note 5.

[24] Gilad Edelman, *Facebook and Twitter Want to Keep the Justice System Stacked Against Defendants*, WIRED (June 19, 2020, 7:00 AM), https://www.wired.com/story/facebook-twitter-criminal-justice-stored-communications-act [https://perma.cc/G3JM-FSRT].

[25] Kashmir Hill, *Imagine Being on Trial. With Exonerating Evidence Trapped on Your Phone*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html [https://perma.cc/LC52-VHC4].

[26] Jeffrey D. Stein, Opinion, *Why Evidence Exonerating the Wrongly Accused Can Stay Locked Up on Instagram*, WASH. POST (Sept. 10, 2019, 4:52 PM), https://www.washingtonpost.com/opinions/2019/09/10/why-evidence-exonerating-wrongly-accused-can-stay-locked-up-instagram [https://perma.cc/ZU2L-2BX5].

*Times*,[27] *CBS News*,[28] and the *San Francisco Chronicle*[29] have often bolstered the companies' position — for instance, normalizing the denial of defense access to evidence by analogizing to home searches and seizures;[30] asserting that this construction of the SCA "prevents defense lawyers from using subpoenas to harass witnesses, victims or police officers";[31] and predicting that "a ruling in favor of . . . defendants could flood companies with subpoenas."[32]

The full scale of harm to the truth-seeking process of the courts is difficult to grasp. It is impossible to determine with certainty how many cases are affected by the current consensus view of the SCA because criminal defense subpoenas may be quashed in unpublished opinions, denied in letter traffic between counsel without reaching a judge, or chilled from service in the first place. But the issue is likely substantial. As some indication, the issue reached the California Supreme Court in two different criminal cases in 2020 (both as a matter of first impression)[33] and the United States Supreme Court in a petition for certiorari that same year;[34] it has triggered rulings by the Second Circuit,[35] the District of Columbia Court of Appeals,[36] and the Supreme Court of

---

[27] Rebecca Wexler, Opinion, *How Data Privacy Laws Could Make the Criminal Justice System Even More Unfair*, L.A. TIMES (July 31, 2019, 3:00 AM), https://www.latimes.com/opinion/story/2019-07-30/consumer-data-privacy-laws-crime-defendants-police-instagram [https://perma.cc/LNN5-GVWK].

[28] McNamara, *supra* note 5.

[29] Megan Cassidy, *Facebook, Twitter Hold Evidence that Could Save People from Prison. And They're Not Giving It Up*, S.F. CHRON. (Jan. 23, 2020, 2:06 PM), https://www.sfchronicle.com/crime/article/Facebook-Twitter-hold-evidence-that-could-save-14990176.php [https://perma.cc/X56X-B8NN].

[30] *Id.* (quoting a professor analogizing a criminal defense subpoena seeking a third party's communications from a technology company to a criminal defendant breaking into a third party's home to search for evidence).

[31] Hill, *supra* note 25.

[32] Trisha Thadani, *Defenders May Use Public Social Media Posts in Trial, Court Says*, S.F. CHRON. (May 24, 2018, 4:42 PM), https://www.sfchronicle.com/business/article/Defenders-may-use-public-social-media-posts-in-12941962.php [https://perma.cc/M5VF-XHV8].

[33] *See* Joyce E. Cutler, *Court to Scrutinize Social Media Posts in California Murder Case*, BLOOMBERG L. (June 10, 2020, 9:02 PM), https://news.bloomberglaw.com/us-law-week/court-to-scrutinize-social-media-posts-in-california-murder-case [https://perma.cc/LXS2-5MKD]; *see also* Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 753 (Cal. 2018). The California Supreme Court issued a ruling in one case, *see* Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020), but remanded the second case for reconsideration in light of that opinion, *see* Facebook, Inc. v. S.C. (*Hunter*), 474 P.3d 635 (Cal. 2020).

[34] Petition for a Writ of Certiorari, *supra* note 7, at ii. The cert petition was denied. Facebook, Inc. v. Superior Ct., 140 S. Ct. 2761 (2020).

[35] United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015).

[36] Facebook, Inc. v. Wint, 199 A.3d 625, 632 (D.C. 2019).

Oregon,[37] among other courts throughout the nation.[38] As another indication of scale, law enforcement and other government entities within the United States served Facebook with 35,856 unique search warrants implicating 55,002 accounts, and Google with 19,783 unique search warrants implicating 28,865 accounts, in just the period from January to June 2020.[39] If criminal defense subpoenas, when properly enforced, were to amount to even a fraction of these numbers, the impact for defendants could be profound. For reference, the total number of criminal cases pending as of March 31, 2019, in all federal district courts combined was 82,443.[40]

Despite an overdue national reckoning with criminal justice reform, the increasing quantity of relevant digital evidence in the hands of technology companies, and a robust, longstanding scholarly debate on other aspects of the SCA,[41] the legal literature has almost entirely overlooked the SCA's treatment of criminal defense subpoenas.[42] Those scholars

---

[37] State v. Bray, 422 P.3d 250, 256 (Or. 2018).

[38] *See* United States v. Nix, 251 F. Supp. 3d 555, 559 (W.D.N.Y. 2017); United States v. Wenk, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017); State v. Johnson, 538 S.W.3d 32, 70 (Tenn. Crim. App. 2017).

[39] *See Overview*, FACEBOOK: TRANSPARENCY, https://transparency.facebook.com/government-data-requests/country/US [https://perma.cc/NT57-KZVU]; *Global Requests for User Information*, GOOGLE: TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview [https://perma.cc/NML2-QQ5G].

[40] *Table D Cases — U.S. District Courts — Criminal Federal Judicial Caseload Statistics (March 31, 2019)*, U.S. CTS., https://www.uscourts.gov/statistics/table/d-cases/federal-judicial-caseload-statistics/2019/03/31 [https://perma.cc/QT6N-TLPD]. Of course, most criminal prosecutions occur in state courts, but the number of pending federal criminal cases is a helpful comparator for understanding the scope of this issue.

[41] *See, e.g.*, Ryan Calo, Response, *Communications Privacy for and by Whom?*, 162 U. PA. L. REV. ONLINE 231, 233 & n.15 (2014) (response to Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373 (2014)) (arguing that Professor Orin Kerr inadequately considered "nongovernmental access to contents of communications," *id.* at 233 n.15 (quoting Kerr, *supra*, at 400)); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) [hereinafter Kerr, *User's Guide*]; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).

[42] There are two welcome exceptions to this general oversight in the literature. Marc Zwillinger and Christian Genetski introduced the issue in a 2007 article, drawing on their own litigation experience in the U.S. Department of Justice to observe, even at that early date, "how frequently public defender's offices, private criminal counsel, and even pro se defendants" attempted to serve subpoenas that were blocked by the SCA. Zwillinger & Genetski, *supra* note 10, at 571. Professors Joshua Fairfield and Erik Luna also discussed the issue in significant depth in a 2014 article, arguing to expand defendants' access to exculpatory evidence through court-ordered consent to disclosures and by narrowly construing the types of companies to which the SCA applies. Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1057–64 (2014). This Article is indebted to the thoughtful commentary in both of these prior works. *See also* Brendan Sasso, *Digital Due Process: The Government's Unfair Advantage Under the Stored Communications Act*, 8 VA. J. CRIM. L. 35 (2020).

For practitioners writing on this issue, see Colin Fieman & Alan Zarky, *When Acquittal Is Just a Tweet Away: Obtaining Historical Social Media Evidence from Service Providers that Use*

who have addressed the issue have generally agreed with the current case law, concluding that the text of the SCA creates an "unequivocal"[43] bar on criminal defense subpoenas "under any circumstances,"[44] and that defendants' prospects for a successful statutory interpretation challenge are "minimal at best."[45]

This Article takes a different approach. The discussion begins in Part I with a puzzle: twenty-first-century courts evaluating the SCA internet privacy law have construed it to block subpoena power, but nineteenth-century courts evaluating similar telegraph privacy laws construed similar statutory texts to yield to subpoenas. The Article argues that nineteenth-century courts reached the correct result because they understood a key point that twenty-first-century courts have overlooked: construing a statute to block subpoena power creates an evidentiary privilege. Part II plays out that point in current doctrine. It explains how federal privacy laws interact with the Federal Rules of Evidence (FRE) to produce privileges and presents a novel doctrinal analysis of the special rules of statutory interpretation that control such interactions. In the process, it identifies a previously unrecognized federal circuit split on a question that is ripe for Supreme Court review: What type of statutory language is required before courts should presume that Congress intended a statute to abrogate its legislatively crafted subpoena and discovery rules, and undermine the truth-seeking process of the courts? This Article argues that, regardless of how the current federal circuit split is ultimately resolved, the statutory interpretation rules for privileges should prohibit courts from construing the SCA to block criminal defense subpoenas.

Part III considers the policy implications of these doctrinal claims. It argues that correcting the erroneous case law on the SCA privilege would impose minimal costs to privacy while eliminating an apparently unjustified subsidy that courts have supplied to technology companies

---

*the SCA as a Shield*, THE CHAMPION, Nov. 2015, at 26; Donald E. Landis, Jr., *MySpace.com: Discovery Issues in the 21st Century*, CAL. DEF., Winter 2008–2009, at 37; Joshua Lipshutz & Michael Holecek, Opinion, *The Criminal Defense Bar Wants Access to Your Emails*, NAT'L L.J. (Feb. 27, 2019, 1:54 PM), https://www.law.com/nationallawjournal/2019/02/27/the-criminal-defense-bar-wants-access-to-your-emails [https://perma.cc/77HL-SXED]; and Stephanie Lacambra, *A Constitutional Conundrum that's Not Going Away — Unequal Access to Social Media Posts*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (May 31, 2018), https://www.eff.org/deeplinks/2018/05/ca-supreme-court-leaves-scales-tipped-prosecutions-favor-defense-gets-access [https://perma.cc/4FAH-6AS8].

[43] Zwillinger & Genetski, *supra* note 10, at 593.

[44] *Id.* at 572.

[45] *Id.* at 593; *see also* Fairfield & Luna, *supra* note 42, at 1056–64 (offering alternate readings of section 2702(b)'s enumerated exceptions to cover some criminal defense subpoenas, and reiterating the consensus view that "the statute does not inherently permit an exception for response to a court subpoena," *id.* at 1058).

and their data-mining markets. The result would serve the shared interest of prosecutors, defendants, the courts, and the public in safeguarding the truth-seeking process of the judiciary. Meanwhile, the current consensus view of the SCA creates a vastly overbroad, outlier privilege for an entire *medium* of communication. Suppressing evidence from the truth-seeking process of the judiciary solely because of its means of transmission, without regard to the sensitivity of the subject matter or the communicants' expectations of confidentiality, is both unprecedented and unwise.

Broadly, this Article seeks to contribute to theorizing the relationship between information privacy law, confidentiality law, and privilege law. It joins recent privacy law scholarship focusing on the law of confidentiality[46] and recent evidence law scholarship focusing on evidence rules outside the four corners of the FRE.[47] The Article also aims to contribute to privacy, criminal procedure, and surveillance studies scholarship by adding consideration of criminal defense investigations to these fields' more traditional focus on law enforcement investigations.[48]

## I. THE INTERNET AND THE TELEGRAPH

This Part presents a puzzle about the internet and the telegraph. Internet and telegraph communications share a number of key features that implicate analogous privacy policy concerns. As a result, each technology inspired similar privacy laws that imposed confidentiality requirements on the communication service provider. Yet, while twenty-first-century courts have nearly uniformly construed the confidentiality provision in the SCA internet privacy law to block subpoenas, nineteenth-century courts took the opposite approach and construed confidentiality provisions in telegraph privacy statutes to yield to subpoenas. How and why did these outcomes diverge? In attempting to answer this question, the following discussion both introduces the current consensus judicial construction of the SCA and demonstrates that it is not inevitable.

---

[46] This Article is especially indebted to Professors Neil Richards and Daniel Solove. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 144–45 (2007); *see also* PRINCIPLES OF THE L.: DATA PRIVACY § 1 (AM. L. INST. 2019) (incorporating the law of confidentiality into data privacy principles).

[47] *See, e.g.*, Bennett Capers, *Evidence Without Rules*, 94 NOTRE DAME L. REV. 867, 869 (2018) (identifying dress, courtroom occupancy, and race *as evidence* that is unregulated — and unacknowledged — by the Rules of Evidence); John Leubsdorf, *Fringes: Evidence Law Beyond the Federal Rules*, 51 IND. L. REV. 613, 615 (2018) (arguing for increased scholarly and pedagogical attention to evidence rules not codified in the FRE).

[48] *See, e.g.*, Julie E. Cohen, *Studying Law Studying Surveillance*, 13 SURVEILLANCE & SOC'Y 91 (2015), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/law/lawsurv [https://perma.cc/FV2T-C9UP].

### *A. The Puzzle*

With both the internet and the telegraph, users send the contents of their communications through intermediary service providers, such as Facebook or the Western Union Telegraph Company.[49] Today, many internet service providers store copies of communications contents as part of a broader data-driven business strategy.[50] Historically, many telegraph service providers also stored copies of the messages they transmitted, not for data analytics but to protect themselves from allegations of faulty transmission.[51] Message retention, in turn, creates a risk that service providers might disclose the contents inappropriately, threatening privacy.[52]

During the years following widespread adoption of the two technologies, policymakers and courts considered this threat to privacy and raised parallel follow-on concerns.[53] For instance, some worried that the threat to privacy might chill adoption of a valuable new communications technology.[54] Others worried that people would be forced to

---

[49] *See* Richards & Solove, *supra* note 46, at 140.

[50] *See generally* JULIE E. COHEN, BETWEEN TRUTH AND POWER (2019).

[51] *See* T.M. Cooley, *Inviolability of Telegraphic Correspondence*, 18 AM. L. REG. 65, 66 (1879).

[52] While internet and telegraph communications share this key feature of service providers that routinely store copies of the contents of messages transmitted through their networks, postal mail and telephone communications generally do not. *See* O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 86 (Ct. App. 2006). Hence, postal mail and telephone privacy statutes are less relevant to the focus of this Article: criminal defense subpoenas to technology companies for *stored* electronic communications contents. Nonetheless, it is worth mentioning that no statute restricts criminal defense subpoenas for mail stored in private facilities. *Cf.* Jeffrey Paul DeSousa, Note, *Self-Storage Units and Cloud Computing: Conceptual and Practical Problems with the Stored Communications Act and Its Bar on ISP Disclosures to Private Litigants*, 102 GEO. L.J. 247, 257 (2013) (observing that "courts have permitted civil discovery of data and documents within storage units in response to . . . third-party subpoenas"). Nor does any statute bar criminal defense subpoenas for the stored contents of telephone communications. To the contrary, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), Pub. L. No. 90-351, 82 Stat. 223 (codified as amended in 18 U.S.C. §§ 2510–2521, 42 U.S.C. § 605), expressly authorizes any person to disclose the stored contents of authorized wiretap materials in court. *See* 18 U.S.C. § 2517(3). Similarly, the Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended in scattered sections of 47 U.S.C.), expressly authorized subpoenas to telephone companies seeking the contents of communications that were "known to employes of the carrier." Nardone v. United States, 302 U.S. 379, 381 (1937). For a detailed examination of postal mail and telephone privacy statutes as they pertain to criminal defense investigations, see Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. (forthcoming 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3428607 [https://perma.cc/T9EY-ZS5Z].

[53] For a discussion of the privacy concerns raised by the rise of the telegraph, see Richards & Solove, *supra* note 46, at 144–45.

[54] *See* Cooley, *supra* note 51, at 70–71; *see also* CONG. RSCH. SERV., R44036, STORED COMMUNICATIONS ACT 5 (2015), https://fas.org/sgp/crs/misc/R44036.pdf [https://perma.cc/Z9QZ-RQKF].

sacrifice their privacy involuntarily to use a technology that was indispensable to modern life.[55] Legislators in both cases responded to these concerns by enacting privacy laws.

With regard to the internet, Congress enacted the SCA in 1986.[56] The SCA's text contains a broad confidentiality provision that generally restricts electronic communication service providers from disclosing the contents of stored communications, and then enumerates a series of express exceptions for permissible disclosures while remaining silent on subpoenas from nongovernmental entities, including criminal defense counsel.[57] In enacting this law, Congress was concerned with invasions of privacy by both private entities and the government.[58] Hence, the SCA not only restricts service providers from disclosing their users' private communications contents,[59] but also prevents private entities from accessing such communications contents without authorization[60] and establishes a detailed statutory framework controlling the various types of legal process that governmental entities must use to obtain different categories of information — from basic subscriber information, to noncontent records such as routing data, to the contents of electronic communications.[61] There is no mention of criminal defense subpoenas anywhere in the SCA's statutory text and virtually no indication in the SCA's legislative history that Congress ever considered them, much less intended to bar them without qualification.[62]

Nineteenth-century state legislatures also passed privacy statutes in response to concerns that telegraph service providers might improperly

---

[55] *See* S. REP. NO. 99-541, at 3 (1986); Cooley, *supra* note 51, at 71.

[56] CONG. RSCH. SERV., *supra* note 54, at 1. The SCA is widely criticized as tied to obsolete technology and deeply outdated. *See, e.g.*, *id.* (observing criticism that the SCA "has outlived its usefulness in the digital era").

[57] Specifically, the SCA states that "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," 18 U.S.C. § 2702(a), and then enumerates nine express exceptions for permissible disclosures, including "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient," *id.* § 2702(b)(1)–(9).

[58] *See* S. REP. NO. 99-541, at 3 (noting concern with privacy invasions from nongovernmental entities); Kerr, *User's Guide*, *supra* note 41, at 1209–13 (noting that, when Congress enacted the SCA, it was motivated in significant part by concerns that the structure of the internet might undermine Fourth Amendment protections from government searches and seizures of communications transmitted through the then-novel technology).

[59] *See* CONG. RSCH. SERV., *supra* note 54, at 3 (describing the SCA as containing "a broad prohibition against providers *voluntarily* sharing customers' communications with the government or others" (emphasis added)).

[60] *See* 18 U.S.C. § 2701.

[61] *See id.* § 2703.

[62] *See infra* pp. 2776–78 (discussing legislative history).

disclose stored communications contents.[63] As with the SCA, many of these statutes contained broad confidentiality provisions that generally restricted telegraph service providers from disclosing the contents of communications, and then enumerated express exceptions for permissible disclosures while remaining silent on subpoenas.[64] For instance, Florida's telegraph privacy statute in force in 1872 stated:

> No officer or person in the employ of any telegraph company . . . shall disclose to any person other than the person to whom any telegraphic message may be directed, or in any manner make known to any other person any part of the contents of any communication . . . [except] to the partner, confidential clerk, or family of any person to whom such message may be directed.[65]

Other telegraph privacy statutes included a broad confidentiality provision with no express exceptions whatsoever, or a sole exception for disclosure to the addressee.[66] A few contained an express exception for

---

[63] *See, e.g.*, Henry Hitchcock, *The Inviolability of Telegrams*, 5 S. L. REV. 473, 495 (1879); Richards & Solove, *supra* note 46, at 144–45. Confidentiality was a significant concern for telegraph users, who devised cipher codes for both efficiency and secrecy purposes. *See generally* Steven M. Bellovin, Compression, Correction, Confidentiality, and Comprehension: A Look at Telegraph Codes 11–12 (June 5, 2020) (unpublished manuscript), https://www.cs.columbia.edu/~smb/papers/codebooks.pdf [https://perma.cc/MU7L-YZTB].

[64] As examples, Illinois's telegraph privacy statute in force in 1874 stated: "[A]ll persons employed in transmitting messages by telegraph . . . who shall make known the contents of a message to any person other than the one to whom it is addressed, or his agent, shall be deemed guilty of a misdemeanor." ILL. REV. STAT. ch. 134, § 7 (1874). Iowa's statute in force in 1873 stated: "Any person employed in transmitting messages by telegraph . . . [who] makes known the contents of any message sent or received to any person except him to whom it is addressed, or to his agent or attorney, is guilty of a misdemeanor." IOWA CODE § 10.1328 (1873). Wisconsin's statute of 1872 stated: "If any [telegraph employee] shall reveal the contents of any private message to any other person than the one to whom it is directed, or to his attorney or agent, it shall be deemed a misdemeanor." WIS. STAT. § 74.19 (1872). Rhode Island's statute of 1872 stated: "[E]very employee of any telegraphic company who shall disclose the contents or purport of any private telegraphic message to a person not authorized to receive the same, shall be fined." 30 R.I. GEN. LAWS § 30-230-36 (1872). California's Act of April 18, 1862, ch. 262, 1862 Cal. Stat. 288 (codified as amended in scattered sections of CAL. PUB. UTIL. CODE), barred telegraph service providers from "willfully divulg[ing], to any other person than the party from whom the same was received, or to whom the same is addressed, or his agent or attorney, any message." *Id.* § 1. New Jersey's Act of March 30, 1855, ch. 195, 1855 N.J. Laws 544 (codified as amended at N.J. STAT. ANN. § 48:17 (2021)), stated:

> [I]t shall not be lawful for any person connected with any line of telegraph . . . to use or cause to be used, or make known or cause to be made known, the contents of any despatch . . . without the consent or direction of either the party sending or receiving the same; and all despatches . . . shall be so transmitted without being made public, or their purport in any manner divulged.

*Id.* § 1.

[65] FLA. STAT. § 50.10 (1872).

[66] For instance, Louisiana's telegraph privacy statute of 1870 stated, without exception: "Any [telegraph employee] . . . who shall reveal, make use of or make public, any dispatch or message, shall, on conviction, be fined." LA. REV. STAT. § 3763 (1870). Pennsylvania's Act of March 31, 1860, No. 374, 1860 Pa. Laws 382 (codified as amended in scattered sections of PA. CONS. STAT.), stated without exception: "If any . . . person, who may be engaged in any telegraph line, shall use,

subpoenas or disclosures "to courts of justice,"[67] but the majority lacked any mention of compliance with judicial process or subpoenas.[68]

The puzzle in this story is about what happened when those privacy statutes clashed with the truth-seeking interests of the judiciary. With both the internet and the telegraph, conflicts arose between litigants who sought to subpoena service provider intermediaries for the contents of stored communications, and service providers who asserted that the governing privacy statute exempted them from complying with those subpoenas. To date, twenty-first-century courts have resolved that clash in favor of the service providers, construing the SCA's confidentiality provision to block judicial compulsory process.[69] Nineteenth-century courts did the opposite, construing telegraph privacy statutes to yield to subpoenas.[70]

The following sections examine the judicial reasoning in each instance. Of course, the internet and the telegraph are not perfectly analogous, either technically or socially.[71] And courts construing the SCA

---

or cause to be used, or make known, or cause to be made known, the contents of any dispatch . . . such person shall be guilty of a misdemeanor." *Id.* § 72. And in Minnesota, a telegraph employee who "willfully divulge[d], to any but the persons for whom it was intended, the contents of a telegraphic message" was punishable by fine and up to six months' imprisonment. MINN. PENAL CODE tit. 15, ch. 12, § 482 (1886).

67 Indiana imposed fines for "[t]he disclosure of messages by any employé of the company except to courts of justice." WILLIAM L. SCOTT & MILTON P. JARNAGIN, A TREATISE UPON THE LAW OF TELEGRAPHS 471 (Boston, Little, Brown, & Co. 1868). Missouri's civil liability statute contained no such exception, but its related misdemeanor statute excepted disclosures "to a court of justice." *See Ex parte* Brown, 7 Mo. App. 484, 491 (Ct. App. 1879) (emphasis omitted) (observing exception in misdemeanor statute but not in civil statute), *aff'd*, 72 Mo. 83 (1880). California's statute was revised in 1880 to add an exception to criminal liability for disclosures directed "by the lawful order of a court." *In re* Storror, 63 F. 564, 566 (N.D. Cal. 1894).

68 *See supra* notes 64–66. Writing in 1879, Henry Hitchcock identified seventeen states with telegraph privacy statutes that were facially silent as to judicial process, including five with entirely unqualified confidentiality rules and twelve with confidentiality rules that were somewhat qualified in that they applied solely to "wilful," "intentional," or "unlawful" disclosures. Hitchcock, *supra* note 63, at 499. He identified another three states as having telegraph privacy statutes that expressly subjected information to judicial process: Indiana, Missouri, and Pennsylvania. *Id.* at 496–98. Indiana's clearly did. *See* SCOTT & JARNAGIN, *supra* note 67, at 471. But the situation in the other two states is more complicated. Missouri's criminal telegraph privacy statute expressly authorized disclosures "to a court of justice," but its civil telegraph privacy statute (at issue in *Ex parte Brown*) was facially silent on disclosures pursuant to judicial process. *Brown*, 7 Mo. App. at 491. Meanwhile, the 1851 version of Pennsylvania's telegraph privacy statute was facially silent as to judicial process, but after a court nonetheless construed it as not creating a privilege to block judicial process, *see infra* note 140 and accompanying text, the statute was amended in 1855 to expressly subject information to judicial process in certain circumstances, *see* Act of May 8, 1855, No. 549, 1855 Pa. Laws 531.

69 *See infra* notes 72–106 and accompanying text (detailing cases).

70 *See infra* notes 132–141 and accompanying text (detailing cases).

71 *Cf.* Jack M. Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 46 (2015) (arguing against formalist approaches to law and technology that focus on essential features of a technology, and instead focusing "on what features of social life the technology makes newly *salient*").

today are hardly bound by nineteenth-century views of statutory construction. Nonetheless, comparing the SCA cases to their telegraph predecessors should help to unsettle any expectations that current judicial interpretations of the SCA are correct merely because they are widespread.

### *B. The Stored Communications Act*

Diving into the legal weeds, courts construing the SCA to unqualifiedly block criminal defense subpoenas have relied heavily on the *expressio unius est exclusio alterius* principle of statutory construction.[72] Section 2702(a) of the SCA imposes a broad confidentiality rule mandating that electronic communication service providers "shall not knowingly divulge to any person or entity the contents of a communication."[73] Section 2702(b) then enumerates nine exceptions for permissible disclosures, including disclosures to law enforcement, while remaining facially silent on criminal defense subpoenas.[74] According to *expressio unius* reasoning, the SCA's list of express exceptions for certain permissible disclosures shows that Congress knew how to write such exceptions, and thus courts should presume that it intended to exclude those not mentioned.[75] Since Congress did not write an express exception for disclosures pursuant to criminal defense subpoenas, courts should not read in an implied exception for those disclosures. Judicial restraint, the argument goes, counsels courts against "lightly engraft[ing] exceptions to plain statutory language without a clear warrant to do so."[76] Nor has the fact that the confidentiality rule in section 2702 is titled "[v]oluntary disclosure of customer communications or records" swayed the courts; to date, judges have rejected the position that disclosures compelled by subpoena are involuntary and thus not prohibited by section 2702(a).[77]

---

[72] *See, e.g.*, Facebook, Inc. v. Wint, 199 A.3d 625, 632 (D.C. 2019).

[73] 18 U.S.C. § 2702(a).

[74] *See id.* § 2702(b).

[75] *Cf.* United States v. Johnson, 529 U.S. 53, 58 (2000). Courts have articulated two versions of the *expressio unius* argument for the SCA. First, section 2702(b) of the SCA enumerates exceptions for authorized disclosures, none of which applies to private litigants' subpoenas. 18 U.S.C. § 2702(b); *see* O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 86 (Ct. App. 2006). And second, section 2703 of the SCA also authorizes disclosures in response to subpoenas served by government entities, *but see* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (noting that commercial internet service providers cannot be compelled to turn over subscriber emails to the government under the SCA if the government has not obtained a warrant), without addressing subpoenas served by anyone else, 18 U.S.C. § 2703; *see* State v. Bray, 422 P.3d 250, 255–56 (Or. 2018).

[76] *O'Grady*, 44 Cal. Rptr. 3d at 86.

[77] *See, e.g.*, *Wint*, 199 A.3d at 628–29. Note that titles and headings generally carry little weight in statutory construction, although they are relevant. *See id.* *But see* Facebook, Inc. v. Superior Ct. (*Touchstone*), 223 Cal. Rptr. 3d 660, 665 (Ct. App. 2017) ("[T]he language of section 2702(a)(1)

This view that the SCA unqualifiedly bars criminal defense subpoenas for communications contents rests on "a seemingly settled body of" federal district court and state appellate court opinions.[78] This construction of the statute is often credited to *O'Grady v. Superior Court*,[79] a 2006 California appellate opinion concerning a civil matter in which Apple sought to subpoena an email service provider for a journalist's communications with an anonymous source who had allegedly leaked Apple's trade secrets.[80] Apple argued that the court should read an implicit exception for civil subpoenas into the statute because nothing in the legislative history of the SCA supports the conclusion that Congress intended to preempt civil subpoena power.[81] The court disagreed, holding instead that "there is no pertinent ambiguity in the language of the statute. It clearly prohibits any disclosure of stored email other than as authorized by enumerated exceptions."[82] The court further reasoned that silence in the SCA's legislative history on this issue "suggests an intent to protect the privacy of stored electronic communications *except where* legitimate law enforcement needs justify its infringement."[83] The ironic origin story of the current SCA subpoena bar, then, is that Apple failed to identify the leaker of its trade secrets and, in the process, unwittingly protected its competitors from a host of administratively challenging subpoenas.

Most federal circuits and state high courts have yet to address this issue. But of the five such courts that have weighed in to date, four agreed with *O'Grady* that SCA section 2702 blocks judicial subpoenas served by nongovernmental litigants without qualification. These courts are the Second Circuit,[84] the California Supreme Court,[85] the

---

and (2) broadly prohibits providers from *voluntarily* sharing subscribers' communications . . . ." (emphasis added)).

78 PPG Indus., Inc. v. Jiangsu Tie Mao Glass Co., 273 F. Supp. 3d 558, 560 (W.D. Pa. 2017). For federal district court and state appellate court rulings on this issue, see *Wint,* 199 A.3d at 629 (collecting criminal subpoena cases); and *PPG Indus.*, 273 F. Supp. 3d at 560–61 (collecting civil subpoena cases).

79 44 Cal. Rptr. 3d 72.

80 *See id.* at 81. Though Apple was attempting to discover the identity of a communicant, which is arguably noncontent information and hence not implicated by SCA section 2702(a), the subpoenas sought "[a]ll *documents relating to* the identity of any person or entity who supplied information regarding an unreleased Apple product code-named 'Asteroid.'" *Id.* at 89–90. The court reasoned that "*any* affirmative response" to those subpoenas would necessarily disclose contents by revealing the existence and author of communications "relating to Asteroid." *Id.* at 90.

81 *See id.* at 85, 87.

82 *Id.* at 86.

83 *Id.* at 87.

84 United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015).

85 Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728 (Cal. 2018). The court allowed only that nongovernmental litigants may access "communications that were configured by the registered user to be public." *Id.*

District of Columbia Court of Appeals,[86] and the Oregon Supreme Court.[87] The Ninth Circuit, in contrast, has presumed in dicta that the SCA yields to otherwise valid judicial compulsory process.[88]

Remarkably, courts construing section 2702 as unqualifiedly blocking criminal defense subpoenas have imported *O'Grady*'s reasoning wholesale from civil to criminal cases, despite the substantial differences in underlying subpoena power and constitutional overtones.[89] In 2017, for instance, a California appeals court held that interpreting the SCA to bar a criminal defendant's subpoena to Facebook did not violate due process, despite the fact that similar legal process is "routinely used as a sword by the prosecution and government."[90] In 2018, the California Supreme Court presumed that criminal defendants' pretrial subpoenas are unenforceable under the SCA "with respect to communications . . . [that are] configured by the registered user to be restricted."[91] In 2019, the District of Columbia Court of Appeals reversed a contempt judgment against Facebook for refusing to comply with a criminal defendant's subpoena, holding that the SCA's enumerated exceptions "comprehensively address the circumstances in which providers may disclose covered communications [and] . . . do not include complying with

---

[86] Facebook, Inc. v. Wint, 199 A.3d 625, 628–29 (D.C. 2019).

[87] State v. Bray, 422 P.3d 250, 256 (Or. 2018).

[88] In *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the defendants had obtained the plaintiffs' email contents by subpoenaing the NetGate technology company; however, a district judge found that the subpoena violated the Federal Rules of Civil Procedure. *Id.* at 1071–72. The Ninth Circuit held that the subpoena did not constitute "authorization" to access the emails under section 2701 because the subpoena was "patently unlawful." *Id.* at 1072; *see id.* at 1073–75. Crucially, the subpoena was unlawful not because it violated section 2702(a), but rather because it was overbroad in violation of the rules of procedure. *Id.* at 1071–72. The court reasoned that the "subpoena's falsity [under the rules of procedure] transformed the access from a bona fide state-sanctioned inspection into private snooping." *Id.* at 1073. The court thus properly presumed that accessing the emails from NetGate via a *lawful* subpoena would have been a "bona fide state-sanctioned inspection," and thus authorized by the SCA. The Ninth Circuit explained that the subpoena at issue in that case violated the SCA because "it would not defeat a trespass claim in analogous circumstances." *Id.* Lawful subpoenas do defeat trespass claims. *See, e.g.*, FED. R. CIV. P. 45(c) ("A subpoena may command . . . inspection of premises at the premises to be inspected."). Hence, under the Ninth Circuit's reasoning, the SCA does not impede a lawful subpoena. *But cf.* Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 728 (9th Cir. 2011) (describing *Theofel* as holding "that a civil subpoena to plaintiff's internet service provider violated the [SCA]," without explaining that *Theofel*'s holding was based on that particular subpoena's overbreadth, not on any SCA impediment to subpoenas generally).

[89] *See generally* MARK J. MAHONEY, THE RIGHT TO PRESENT A DEFENSE 28–44 (2016), https://www.harringtonmahoney.com/content/Publications/Mahoney%20-%20Right%20to%20-Present%20a%20Defense%202017.pdf [https://perma.cc/RUG3-LCU3].

[90] Facebook, Inc. v. Superior Ct. (*Touchstone*), 223 Cal. Rptr. 3d 660, 669 (Ct. App. 2017) (quoting the criminal defendant's argument); *see id.* at 671.

[91] Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728 (Cal. 2018).

criminal defendants' subpoenas."[92] The Second Circuit,[93] the Oregon Supreme Court,[94] the Tennessee Court of Criminal Appeals,[95] and federal district courts in the Western District of New York[96] and the Eastern District of Virginia[97] have all ruled similarly.

The harms to the truth-seeking process of the judiciary are multilayered. The first layer is the flat denial of evidence that is relevant and material to the defense of the criminally accused. In one recent case, a defendant claimed self-defense, alleging that the victim had previously attempted to murder him in a drive-by shooting and then used an Instagram account to harass, threaten, and stalk him for months, keeping him "in constant fear for his life."[98] But when the defendant tried to subpoena Instagram for copies of these communications, Instagram asserted that the SCA exempted it from complying with the subpoena.[99] In Instagram's view, the SCA allowed the defendant to subpoena the records . . . just not from Instagram.[100] He would have to subpoena the account holder directly, meaning, in this case, the man who was allegedly trying to kill him.

This case is hardly an isolated example. In another recent case, two defendants sought impeachment material for a key prosecution witness, and the trial judge determined that directing a subpoena to the witness herself would not be "viable for obtaining [the impeachment] information in the form and the manner, and [with] the authenticity guarantees that the defendants would need it."[101] Nonetheless, the SCA barred the defendants from obtaining the information from Facebook, Twitter, and Instagram.[102] In another recent case, the SCA blocked a criminal defense subpoena to Facebook notwithstanding the trial judge's finding that notifying the account holder directly could "lead to tampering with

---

92 Facebook, Inc. v. Wint, 199 A.3d 625, 628 (D.C. 2019).

93 *See* United States v. Pierce, 785 F.3d 832, 842 (2d Cir. 2015).

94 *See* State v. Bray, 422 P.3d 250, 256 (Or. 2018).

95 *See* State v. Johnson, 538 S.W.3d 32, 70 (Tenn. Crim. App. 2017).

96 *See* United States v. Nix, 251 F. Supp. 3d 555, 559 (W.D.N.Y. 2017).

97 United States v. Wenk, 319 F. Supp. 3d 828, 829 (E.D. Va. 2017).

98 Opp'n to Instagram Motion, *supra* note 1, at 5; *see id.* at 1 & n.1, 4–6, 8, Exhibit A.

99 *Id.* at 2, 7.

100 *Id.* at 9–10. Notably, Facebook has taken the position that the SCA's "consent" exception, *see* 18 U.S.C. § 2702(b)(3), does not apply to messages directed to a recipient for a time-limited period, such as Facebook posts whose accessibility settings have changed or Instagram messages that "disappear" even while copies may remain on the companies' servers, *see* Facebook, Inc. v. Pepe, 241 A.3d 248, 254 (D.C. 2020); Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 732 (Cal. 2018) (documenting Facebook's interpretation of the law); *see also* David Pierce, *Instagram's New Story Highlights Save Your Disappearing Videos Forever*, WIRED (Dec. 5, 2017, 10:00 AM), https://www.wired.com/story/instagrams-new-story-highlights-save-your-disappearing-videos-forever [https://perma.cc/DF64-LMYU].

101 Transcript of Proceedings at 22, People v. Hunter, Nos. 13035658, 17004548, 13035657 (Cal. Super. Ct. May 1, 2019) (on file with the Harvard Law School Library).

102 *See* Facebook, Inc. v. Superior Ct. (*Hunter*), 259 Cal. Rptr. 3d 331, 332 (Ct. App. 2020).

or destruction of evidence."[103] In another recent case, the SCA blocked a homicide defendant's subpoena for records concerning an individual in witness protection whom the defendant alleged had evidence important to his defense.[104] In another recent case, the SCA blocked a defense subpoena to Facebook seeking impeachment material for a prosecution witness that a judge had deemed relevant and material to the case.[105] In another recent case, the SCA blocked a defense subpoena to Facebook and Twitter seeking potentially exculpatory posts from suspended social media accounts.[106] In another recent case, the SCA blocked a person on death row from subpoenaing GitHub, a company that provides internet hosting services for software development, for the source code in a forensic software system used to analyze evidence at his trial.[107] While it is impossible to know precisely how many defendants are affected by the current case law, it is certainly many more than appear thus far in published appellate opinions.

---

[103] Order for Preservation of Stored Account Content, People v. Touchstone, No. 268262 (Cal. Super. Ct. Mar. 16, 2017) (on file with the Harvard Law School Library); *see* Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 403 (Cal. 2020) (vacating the trial court's denial of Facebook's motion to quash). Note that courts have general authority to issue preservation and nondisclosure orders accompanying criminal defense subpoenas, as at least two state supreme courts have held when considering defense subpoenas and the SCA in particular. *See generally Pepe*, 241 A.3d at 263–64 (acknowledging that, "[g]enerally speaking, criminal defendants 'should be permitted to make an *ex parte* application for pretrial production of documents,'" and discussing standards that apply to defendants' motions for an additional nondisclosure order accompanying such subpoenas (quoting United States v. Sellers, 275 F.R.D. 620, 625 (D. Nev. 2011))); *Touchstone*, 471 P.3d at 399 & n.13 (reviewing *Touchstone* subpoena that included preservation and nondisclosure orders, acknowledging the appropriateness of such preservation orders in certain circumstances by commenting that "after such preservation has occurred (hence presumably addressing concerns about possible spoliation by a social media user)," a court should assess whether "notice to a victim/social media user should be provided," *id.* at 399 n.13, and not otherwise commenting on or prohibiting the issuance of nondisclosure orders); *In re* Holmes v. Winter, 3 N.E.3d 694, 701 (N.Y. 2013) (nondisclosure order to parties).

[104] *See* Defense Counsel's Declaration in Support of Motion to Compel Facebook Inc.'s Compliance with Subpoenas Duces Tecum ¶¶ 11, 14, People v. Baldino, No. 258141 (Cal. Super. Ct. July 15, 2016) (on file with the Harvard Law School Library); Non-party Facebook, Inc.'s Notice of Motion and Motion to Quash Subpoenas Duces Tecum and Authorities in Support, *Baldino*, No. 258141 (Cal. Super. Ct. July 22, 2016) (on file with the Harvard Law School Library) [hereinafter Facebook Motion to Quash]; *see also* E-mail from Jeremy Thornton, Att'y, San Diego Cnty. Pub. Def. Off., to author (Apr. 20, 2021) (on file with the Harvard Law School Library).

[105] Order Denying Facebook, Inc.'s Motion to Vacate Orders and Quash Subpoenas at 3, United States v. Wint, 2015 CFI 7047 (D.C. Super. Ct. 2018), *reprinted in* Petitioner's Rule 8.520(d) Supplemental Brief Regarding *Facebook, Inc. v. Wint* (D.C. 2019) and *Facebook, Inc. v. Superior Court* (*"Hunter III"*) (2020), *Touchstone*, 471 P.3d 383 (No. S245203); *see also* Facebook, Inc. v. Wint, 199 A.3d 625, 633–34 (D.C. 2019).

[106] McNamara, *supra* note 5 (documenting Facebook's and Twitter's reliance on the SCA to refuse to comply with a criminal defense subpoena seeking posts from suspended ISIS social media accounts).

[107] *See* Protective Order, *supra* note 3; Order Denying Colone's Motion, *supra* note 3.

A second-order harm comes from chilling effects. Defense attorneys have reported receiving overbroad default denials from service providers via form letters that improperly cite the SCA content-disclosure bar even when subpoenas seek basic subscriber information, which the SCA unambiguously permits.[108] Challenging these types of overbroad denials costs time and attorney resources, including for informal negotiations between the parties that may take place prior to and apart from litigation over motions to quash. Difficulty obtaining records can deter counsel from seeking such subpoenas at all.[109] Indeed, Facebook and Twitter have been so aggressive in denying criminal defense subpoenas that they argued motions to quash all the way up to both the California Supreme Court and the District of Columbia Court of Appeals advancing the highly questionable positions that — despite express exceptions in the SCA permitting service providers to disclose communications contents to an intended recipient of the message[110] — service providers retain discretion to refuse to comply with criminal defense subpoenas seeking messages that were posted publicly,[111] or initially sent to, but no longer possessed by, the defendant.[112] In both cases the companies ultimately lost,[113] draining time and litigation resources from indigent defendants and their counsel along the way.

Notably, even under current readings of the SCA, criminal defendants and other nongovernmental litigants may still subpoena communications contents from technology companies if the account holder or an intended recipient of a message consents,[114] or subpoena the account holders directly.[115] Courts have relied on the former to eliminate much of the SCA's current sting for *civil* litigants. Civil litigants routinely subpoena opposing parties' communications contents via the SCA consent exception, under the theory that courts' power to manage discovery authorizes judges to compel consent from the litigants before them.[116]

---

[108] Telephone Interview with Hanni Fakhoury, Senior Staff Att'y, Elec. Frontier Found. (Jan. 30, 2019) (on file with the Harvard Law School Library).

[109] *Id.* Defense attorneys may be chilled even from seeking the contents of their own clients' online accounts: if the client has had their device confiscated, been incarcerated without permission to use electronics, and forgotten their account password, counsel may have no way to prove to the company that their client is the account holder or intended recipient of a message.

[110] *See* 18 U.S.C. § 2702(b)(3).

[111] *See* Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 732 (Cal. 2018).

[112] *See* Facebook, Inc. v. Pepe, 241 A.3d 248, 254 (D.C. 2020).

[113] *See Hunter*, 417 P.3d at 728 (rejecting providers' argument that section 2702 "bars disclosure . . . of communications that were configured by the registered user to be public"); *Pepe*, 241 A.3d at 254.

[114] *See* 18 U.S.C. § 2702(b)(3).

[115] *Cf.* Juror Number One v. Superior Ct., 142 Cal. Rptr. 3d 151, 158–59 (Ct. App. 2012). Litigants may also subpoena account holders directly to compel them to obtain their own records from the company and then produce them. *See* Facebook Motion to Quash, *supra* note 104, at 1.

[116] *See* Fairfield & Luna, *supra* note 42, at 1059–60, 1059 nn.493–98, 1060 n.99 (collecting civil cases); *cf.* DeSousa, *supra* note 52, at 265 (discussing *Flagg ex rel. Bond v. City of Detroit*, 252 F.R.D.

But such judicially compelled consent is unavailable to criminal defendants, who necessarily seek the communications of nonparties.[117] Instead of the exceptions aiding criminal defendants, as they have civil litigants, courts have applied the exceptions to make it harder for criminal defendants to successfully subpoena information. For instance, a California appellate court recently held that a criminal defendant had failed to establish constitutional need to subpoena Facebook, Instagram, and Twitter for impeachment evidence from a prosecution witness's accounts because defense counsel could have attempted to identify the witness's contacts, and then subpoena each of those contacts for copies of their communications with that witness.[118]

Meanwhile, criminal defendants may be unable to subpoena account holders directly. Difficulties arise when account holders refuse to comply with the subpoena or withhold consent to a company's production of their communications, cannot be located, reside or are domiciled abroad, are deceased, or have a Fifth Amendment or other privilege against production; or where notifying the users about the investigation could lead to the destruction of or tampering with evidence, flight, witness intimidation, or a threat to life or safety. Indeed, the SCA itself recognizes that such circumstances arise in law enforcement investigations.[119] Criminal defense investigators face many of the same circumstances in which law enforcement may prefer to, and currently can, obtain information from technology companies, rather than from individual account holders.[120] Correcting the case law to eliminate the current SCA subpoena bar would further judicial truth-seeking in those cases.

### *C. Telegraph Privacy Statutes*

The story of the SCA, and current judicial constructions of it to block criminal defense subpoenas, has a foil in the history of the telegraph. Recall that nineteenth-century legislatures also enacted statutes to protect the privacy of communications contents transmitted through service

346 (E.D. Mich. 2008), in which the court ordered the plaintiff to redirect a subpoena to the defendant instead of the provider); Timothy G. Ackermann, *Consent and Discovery Under the Stored Communications Act*, FED. LAW., Nov.–Dec. 2009, at 41, 45.

117 *See, e.g.*, Application for Leave to File Amicus Curiae Brief and Amicus Curiae Brief of Electronic Frontier Foundation in Support of Plaintiff and Petitioner Facebook, Inc. at 5, 12–13, Facebook, Inc. v. Superior Ct., No. 248609 (Cal. Ct. App. May 30, 2013), 2013 WL 2391432, at *5, *12–13. A criminal defendant's opposing party is generally understood as "the People." *But cf.* Jocelyn Simonson, Essay, *The Place of "The People" in Criminal Procedure*, 119 COLUM. L. REV. 249, 252 (2019) (contrasting usage of the phrase "the People" in criminal cases with how marginalized groups actually publicly participate in and organize against the criminal law).

118 Facebook, Inc. v. Superior Ct. (*Hunter*), 259 Cal. Rptr. 3d 331, 339–40 (Ct. App. 2020).

119 *Cf.* 18 U.S.C. § 2705(b) (detailing some such circumstances).

120 *See id.* § 2703; *see also* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 325 (2012).

provider intermediaries.[121] Similar to the SCA, many of these telegraph privacy statutes contained broad confidentiality provisions, and then enumerated express exceptions for permissible disclosures while remaining facially silent as to disclosures pursuant to judicial compulsory process.[122] As a result, nineteenth-century litigants and commentators urged courts to construe the statutes to exempt telegraph companies from complying with subpoenas. In short, they asked courts to read the telegraph privacy statutes just as twenty-first-century courts have read the SCA.

Perhaps the most prominent proponent of this position was Michigan Supreme Court Chief Justice Cooley.[123] Foreshadowing the United States Supreme Court's 2018 reasoning in *Carpenter v. United States*[124] that carrying a cell phone "is indispensable to participation in modern society,"[125] Chief Justice Cooley asserted that the "exigencies" of modern life necessitated the use of telegrams, and thus such use was not "a matter of mere choice."[126] Yet Chief Justice Cooley went beyond *Carpenter*'s recognition of Fourth Amendment protection for cell-site location records; he argued that telegraphs should be shielded from subpoena by governmental and private litigants alike, and thus exempted entirely from "the process of the courts."[127] Specifically, Chief Justice Cooley read telegraph privacy statutes not merely to impose "penalties" for unauthorized disclosures, but also to prevent "judicial command."[128] In his view, judges lacked power to compel the disclosure of private messages relayed "under a confidence imposed by the law."[129]

Chief Justice Cooley failed. Courts repeatedly rejected the position he espoused and instead enforced subpoenas served on telegraph companies.[130] The absence of express textual exceptions to permit disclosures made in response to subpoenas did not matter to these courts; they

---

[121] *See supra* note 63 and accompanying text.

[122] *See supra* notes 63–68 and accompanying text.

[123] Chief Justice Cooley's treatise on torts recognized the concept of a legal right "to be let alone" that Samuel Warren and Louis Brandeis developed in their influential article *The Right to Privacy*. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 & n.4 (1890) (quoting THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888)).

[124] 138 S. Ct. 2206 (2018).

[125] *Id.* at 2220. In *Carpenter*, the Supreme Court relied on this reasoning to deny the government access to cell-site location information under the Fourth Amendment. *See id.*

[126] Cooley, *supra* note 51, at 71.

[127] *Id.*

[128] *Id.* at 73.

[129] *Id.* at 77.

[130] *See* Hitchcock, *supra* note 63, at 473 (describing cases). The case law in the United States was sufficiently uniform on the issue that a superior court in Montreal relied on that uniformity to hold that a similar Canadian telegraph statute, "which declare[d] it a misdemeanor in any operator or employee of a Telegraph Company to divulge the contents of a private despatch, does not apply to the production of telegrams by the Secretary of the Company, in obedience to a subpoena duces

construed the statutory silence to yield to judicial process.[131] Why did these courts not follow the *expressio unius* principles that their twenty-first-century successors would apply?

Nineteenth-century courts responded this way at least in part because they understood a key point that twenty-first-century courts have overlooked: when courts read a statute to block subpoenas, they construe the statute as creating an evidentiary privilege. For instance, the Missouri Supreme Court explained that "[t]he only ground . . . upon which the exemption of telegrams from this process of the court can be placed, is that they are privileged communications."[132] Similarly, the Supreme Judicial Court of Maine rejected a claim "that the telegram was a privileged communication."[133] And a Pennsylvania civil court of common pleas rejected the argument that the state's telegraph privacy statute "classed [telegraphs] with privileged communications, such as those between husband and wife, counsel and client."[134] As one commentator summarized in 1879: "[A]ll these arguments amount simply to the claim that private telegraphic messages . . . constitute a new class of privileged communications. But no statute gives color to any such claim, and the courts have uniformly denied it."[135]

Nineteenth-century courts considering telegraph privacy statutes also recognized the gravity of construing a statute as creating a privilege. In declining to read a telegraph privacy statute in this manner, the Missouri Supreme Court explained that the authority "to compel the production of written as well as oral testimony, seems essential to the very existence and constitution of a court of common law, which . . . could not possibly proceed, with due effect, without them,"[136] and hence concluded that it could not "declare [telegraph communications to be privileged] in the absence of a statute so providing."[137] The

---

tecum." Leslie v. Hervey (1870), 15 L.C. Jur. 9, 9 (Can. Que. Sup. Ct.) (emphasis omitted); *see id.* at 11.

131 For instance, Mississippi's telegraph privacy statute stated that telegraph service providers "shall [not] use, or cause to be used, or make known, or cause to be made known, the contents of any dispatch . . . without the consent or direction of the party sending or receiving the same." MISS. REV. CODE ch. 35, art. 51 (1857). Despite this statutory text, a federal district court in Mississippi determined that a procedurally valid subpoena to a telegraph company would be enforceable. *See* United States v. Hunter, 15 F. 712, 715 (N.D. Miss. 1882) ("When such a subpoena is served upon the person having the possession of the telegram, it is his duty to . . . produce the telegram.").

132 *Ex parte* Brown, 72 Mo. 83, 92 (1880).

133 State v. Litchfield, 58 Me. 267, 268 (1870); *see id.* at 268–69 (holding that "a telegraphic operator is bound to testify to the contents of a telegraphic message," *id.* at 269). The Maine Supreme Judicial Court ruled this way despite Maine's telegraph privacy statute, which imposed civil liability on a telegraph "operator or agent [who] willfully divulges any part of the contents of a private dispatch entrusted to him for transmission or delivery." ME. REV. STAT. tit. 4, ch. 53, § 1 (1871).

134 Henisler v. Freedman, 2 Pars. Eq. Cas. 274, 277 (Pa. Ct. Com. Pl. 1851).

135 Hitchcock, *supra* note 63, at 506.

136 *Brown*, 72 Mo. at 92 (quoting Amey v. Long (1808) 103 Eng. Rep. 653, 658; 9 East 473, 484).

137 *Id.*

court determined that Missouri's telegraph privacy statute did not so provide, declaring that it was "obvious" that the legislature intended the statute to yield to judicial process.[138] The Missouri appellate court below had likewise observed that "the construction of such acts is well settled. It is understood that there is always an exception in favor of legal process."[139] Similarly, a Pennsylvania civil court of common pleas reasoned that:

> If the Legislature had intended to place telegraph communications [on a similar basis as privileged communications, such as those between husband and wife], it would have been easy to have said, that no person connected with any line of telegraph should be permitted to produce a telegraph despatch, or to prove its contents in a court of justice, without the assent of the parties to it.[140]

And as a federal district court in California explained, there was judicial consensus on the conclusion that "even where the statutory prohibition is unqualified, there is always an exception implied in favor of legal

---

[138] *Id.* at 93. In this case, the Missouri Supreme Court construed Missouri's civil confidentiality statute, which stated: "Every telegraph company . . . shall be liable . . . for the disclosure of any of the contents of any private dispatch to any person other than to him to whom it was addressed, or to his agent." MO. ANN. STAT. § 37.13 (Wagner 1872). Despite the statute's textual silence as to disclosures pursuant to judicial process, the court refused to construe the statute as impliedly creating a privilege to block judicial process. *See Brown*, 72 Mo. at 92. The court reasoned in part based on comparison to Missouri's related misdemeanor statute that contained a criminal prohibition on such disclosures and that *did* contain an express exception for disclosures to "a court of justice." MO. ANN. STAT. § 42.51; *see Brown*, 72 Mo. at 93. The court rejected the *expressio unius* logic that, since the legislature knew how to write an express exception for disclosures pursuant to legal process, and did so in the criminal misdemeanor statute, it must have meant to bar such disclosures via silent statutory text in the civil confidentiality statute. Instead, the court adopted the reasoning from the majority appellate opinion below, which quoted the pertinent language from both the criminal and civil statutes, similarly concluded that the purpose of the civil statute was "obvious," explained that "there is always an exception in favor of legal process," and asserted that such "disclosure is the act of the law, not that of the company." *Ex parte* Brown, 7 Mo. App. 484, 492 (Ct. App. 1879).

[139] *Brown*, 7 Mo. App. at 492.

[140] Henisler v. Freedman, 2 Pars. Eq. Cas. 274, 277 (Pa. Ct. Com. Pl. 1851). In this case, the court of common pleas declined to construe Pennsylvania's Act of April 14, 1851, No. 331, 1851 Pa. Laws 612 (codified as amended in scattered sections of PA. CONS. STAT.), as creating a privilege to block subpoenas, where the statute stated:

> [I]t shall not be lawful for any person connected with any line of telegraph . . . to use or cause to be used, or make known or cause to be made known, the contents of any despatch . . . without the consent or direction of either the party sending or receiving the same; and all despatches . . . shall be so transmitted without being made public, or their purport in any manner divulged . . . .

*Id.* § 7. In considering the argument that telegraphs should "be classed with privileged communications," the court commented: "Had such a direct proposition been placed before the Legislature, I cannot think that it would have prevailed." 2 Pars. Eq. Cas. at 277. Shortly after the decision in this case, the Pennsylvania legislature amended the statute to expressly require telegraph companies to preserve telegraph communications contents "and to produce the same in evidence whensoever duly subpoenaed to do so by the individual or individuals . . . sending or receiving a copy of such messages." Act of May 8, 1855, No. 549, § 2, 1855 Pa. Laws 531.

process, since obedience to a subpoena is obligatory upon all."[141] Hence, nineteenth-century courts denied the creation of a privilege from telegraph statutes that contained broad confidentiality provisions and enumerated express exceptions for certain permissible disclosures without mentioning subpoenas.

In sum, privacy concerns pertaining to internet and telegraph communications prompted lawmakers, over a century apart, to enact similar privacy statutes. In both cases, those statutes clashed with the truth-seeking interests of the judiciary. Twenty-first-century and nineteenth-century courts faced with resolving that clash evaluated similar statutory texts, considered parallel legal and policy arguments, and reached opposite results. The remainder of this Article explains why courts today should reverse course and follow the nineteenth-century approach when construing the SCA.

## II. PRIVACY AS PRIVILEGE

This Part presents an original analysis of current doctrine governing statutory privileges and applies that analysis to the SCA. Section A argues that a statute that blocks an ex ante category of relevant evidence from judicial compulsory process suffices to create a privilege. Section B then develops a novel synthesis of the rules that govern when courts must, and must not, construe federal statutes as creating privileges. Put succinctly, judges must not legislate privileges from the bench by reading federal statutes to block judicial process unless a statute's plain text *requires* this result. Courts that have read the SCA to block criminal defense subpoenas have construed ambiguous silence in the statutory text as impliedly creating a privilege, and have done so erroneously.

### *A. Statutory Privileges*

This section begins by broadly describing federal statutory privileges. Recognizing the lack of a general definition of evidentiary privileges in existing legal authorities, it induces a definition from the essential feature of privileges: that they block an ex ante category of relevant information from judicial compulsory process. It then discusses other common features of privileges before contrasting confidentiality with privilege. Finally, the section argues that current judicial constructions of the SCA satisfy the definition of a privilege.

*1. Defining Statutory Privileges.* — In general, the FRE leave privileges to common law development.[142] As prior scholars have noted,

---

[141] *In re* Storror, 63 F. 564, 567 (N.D. Cal. 1894) (quoting JOHN ORDRONAUX, CONSTITUTIONAL LEGISLATION IN THE UNITED STATES 249 (1891)).

[142] FED. R. EVID. 501.

this exceptional departure from the overall codification of evidence law resulted from political controversy. The initial proposed draft of the FRE included a series of privileges: relational privileges for confidential communications between lawyers and clients, psychotherapists and patients, and clergy and penitents, as well as topical privileges for required reports, political votes, trade secrets, state secrets, and the identity of informants.[143] But congressional hearings on the proposed privileges inspired a rush of professional associations seeking additional privileges for their special communications, and responsive allegations that privilege law was being co-opted to enhance professional prestige at the expense of judicial truth-seeking.[144] Congress ducked the debate by removing the proposed privileges from the FRE,[145] kicking privilege law (largely) back to the courts for common law development.[146]

Nonetheless, statutory privileges still exist,[147] even when the statutes appear at first to be unrelated to the FRE. FRE 501 incorporates other federal statutes that create privileges by stating that federal courts' common law authority over claims of privilege does not apply if a federal statute "provides otherwise."[148] Hence, in the words of the Supreme Court, "[i]t is well recognized that a privilege may be created by statute."[149] So, then, what makes a statute a privilege?

Without purporting to provide a comprehensive definition, this section proposes that construing a statute to shield an ex ante category of relevant evidence from judicial compulsory process suffices to create a

---

143 Edward J. Imwinkelried, *Draft Article V of the Federal Rules of Evidence on Privileges, One of the Most Influential Pieces of Legislation Never Enacted: The Strength of the Ingroup Loyalty of the Federal Judiciary,* 58 ALA. L. REV. 41, 43, 47 (2006).

144 *See* 26 KENNETH W. GRAHAM, JR., & ANN MURPHY, FEDERAL PRACTICE & PROCEDURE § 5642 (1st ed.) (Westlaw) (last visited Apr. 10, 2021); Imwinkelried, *supra* note 143, at 48–50; *see also Proposed Rules of Evidence: Hearings Before the Spec. Subcomm. on Reform of Fed. Crim. L. of the H. Comm. on the Judiciary*, 93d Cong. 168, 175 (1973) (statement of Charles R. Halpern & George T. Frampton, Jr., Washington Council of Lawyers).

145 Imwinkelried, *supra* note 143, at 51–52; FED. R. EVID. 501.

146 Imwinkelried, *supra* note 143, at 52–53. However, the Rules Enabling Act, 28 U.S.C. § 2072, maintains special congressional control over privileges, requiring that any "'rule creating, abolishing, or modifying an evidentiary privilege' must be 'approved by [an] Act of Congress.'" Kenneth S. Broun & Daniel J. Capra, *Getting Control of Waiver of Privilege in the Federal Courts: A Proposal for a Federal Rule of Evidence 502*, 58 S.C. L. REV. 211, 218 (2006) (alteration in original) (quoting 28 U.S.C. § 2074(b)).

147 Indeed, codified privileges require special "approval by Act of Congress," unlike other evidence rules that are adopted by the United States Supreme Court pursuant to the Rules Enabling Act. Hon. Sidney A. Fitzwater, Remarks at Panel Discussion: Reinvigorating Rule 502 (Oct. 5, 2012), *in* 81 FORDHAM L. REV. 1533, 1535 (2013).

148 FED. R. EVID. 501. Statutory privileges "cannot be displaced by another rule adopted by the Supreme Court unless that rule has been affirmatively approved by Congress." 23A GRAHAM & MURPHY, *supra* note 144, § 5437.

149 Baldrige v. Shapiro, 455 U.S. 345, 360 (1982).

privilege.[150] Support for this conclusion comes from the relationship between the rules of evidence and those of procedure. The Federal Rules of Civil Procedure entitle parties to discover any "nonprivileged" information that is relevant and proportional to the dispute.[151] Therefore, rules that block an ex ante category of information from discovery for reasons other than relevance or proportionality must be privileges.

The Supreme Court has adopted this reasoning explicitly and repeatedly. In *United States v. Nixon*,[152] the Court stated that the law provides "a right to every [person's] evidence, except for those persons protected by a constitutional, common-law, or statutory privilege."[153] In *Baldrige v. Shapiro*,[154] the Court elaborated that federal civil discovery "provides for access to all information 'relevant to the subject matter involved in the pending action' unless the information is privileged. If a privilege exists, information may be withheld . . . ."[155] The Court then went on to reason that a statute might shield a category of relevant information from discovery if the statute created a privilege.[156] Similarly, in *Hickman v. Taylor*,[157] the Court observed that "limitations [on discovery] come into existence when the inquiry touches upon the irrelevant or encroaches upon the recognized domains of privilege."[158]

Further support comes from leading legal dictionaries and treatises. Black's Law Dictionary defines "privilege" as a "special legal right, exemption, or immunity," and "testimonial privilege" as a "privilege that overrides a witness's duty to disclose matters within the witness's knowledge, whether at trial or by deposition."[159] In *The New Wigmore*, Professor Edward Imwinkelried defines privileges to include statutes

---

[150] It matters that the category of protected information is determined ex ante because trial judges retain discretion to quash legal process on a case-by-case basis. *See, e.g.*, FED. R. CRIM. P. 17(c)(2); FED. R. CIV. P. 26(b) advisory committee's note to 1970 amendment, (b)(1), (c); *id.* 45(d)(3); FED. R. EVID. 611(a); *see also* Hickman v. Taylor, 329 U.S. 495, 512 (1947). These discretionary quashals fall outside the scope of this definition of a statutory privilege.

[151] *See, e.g.*, FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense . . . .").

[152] 418 U.S. 683 (1974).

[153] *Id.* at 709 (emphasis added) (quoting Branzburg v. Hayes, 408 U.S. 665, 688 (1972)).

[154] 455 U.S. 345.

[155] *Id.* at 360 (quoting FED. R. CIV. P. 26(b)(1) (amended 2015)).

[156] *Id.* at 360–61.

[157] 329 U.S. 495 (1947).

[158] *Id.* at 508; *see also* Ass'n for Women in Sci. v. Califano, 566 F.2d 339, 343 (D.C. Cir. 1977) (stating that a party "may obtain discovery regarding any matter, not privileged, which is relevant," *id.* (quoting FED. R. CIV. P. 26(b)(1) (amended 2007)), and because relevance was not contested, determining that "[t]he sole question to be answered, therefore, is whether the forms were privileged").

[159] *Privilege*, BLACK'S LAW DICTIONARY (11th ed. 2019).

that provide "a limited right to protect the confidentiality of certain communications or information . . . in judicial proceedings."[160] In *Federal Practice and Procedure*, Professors Kenneth W. Graham, Jr., and Ann Murphy assert that "a privilege may be inferred from [statutory] language that makes the information immune from process or providing that a person cannot be compelled to reveal it."[161] Similarly, *Weinstein's Federal Evidence* treatise observes that "courts typically construe statutes . . . strictly against the creation of a privilege, to preserve the *access* of the courts and litigants to as much relevant information as is possible."[162] Preserving access to evidence means preserving judicial process. So the *Weinstein's* formulation presumes that construing a statute to block process would create a privilege. When courts construe a statute as blocking an ex ante category of relevant information from valid judicial process, the courts construe that statute as creating an evidentiary privilege.

*2. Common Features of Privileges.* — Beyond the technical definition of privileges, certain common features help to distinguish them from other rules of evidence — specifically, their breadth, power, and extraordinary costs. Whereas most evidence rules apply solely at trial, privileges apply to every stage of a case, from investigations by law enforcement or criminal defense counsel, to grand jury proceedings, to pretrial, trial, and postconviction proceedings.[163] Privileges even shield information from distribution to foreign tribunals.[164] And, unlike most evidence rules, any individual who holds a privilege can intervene to assert it, even if they are not a party to the dispute.[165]

With this breadth comes exceptional power. Privileges block not merely the admissibility of evidence in court but also litigants' ability to compel the production of information for their own review.[166] Privileges can shield information from warrants,[167] subpoenas,[168] and discovery

---

160 EDWARD J. IMWINKELRIED, THE NEW WIGMORE: A TREATISE ON EVIDENCE § 1.3 (3d ed.) (Westlaw) (last accessed Apr. 10, 2021).

161 23A GRAHAM & MURPHY, *supra* note 144, § 5437 (citations omitted).

162 3 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 502A.04 (2d ed.) (LexisNexis) (last accessed Apr. 10, 2021) (emphasis added).

163 *Id.* § 501.02.

164 *See* 28 U.S.C. § 1782.

165 *See, e.g.*, *In re* Grand Jury Subpoena Dated Dec. 17, 1996, 148 F.3d 487, 490 (5th Cir. 1998); *see also* 23A GRAHAM & MURPHY, *supra* note 144, § 5437 n.26.

166 *See* FED. R. EVID. 1101(c) (noting that privilege rules apply "to all stages of a case," which includes discovery); 3 WEINSTEIN & BERGER, *supra* note 162, § 501.02 (stating that the civil procedure rules on privilege apply "at all stages of all actions, cases and proceedings, including discovery proceedings").

167 *See, e.g.*, 18 U.S.C. § 2517(4); Eric D. McArthur, Comment, *The Search and Seizure of Privileged Attorney-Client Communications*, 72 U. CHI. L. REV. 729, 740–44 (2005).

168 FED. R. CIV. P. 45(d)(3)(A)(iii).

orders.[169] Privileged communications may be protected against wiretapping.[170] When executing a warrant requires technical overseizure, as can be the case with electronic data seizures from hard drives or other devices, privileges may require the government to engage in ex post minimization procedures. One such procedure is the use of a "taint team" to purge privileged content prior to delivering the materials to the prosecution team.[171] Put succinctly, privilege protection can be more powerful than torts, contracts, fiduciary duties, or even the Fourth Amendment.

Indeed, multiple authorities characterize privileges as not just powerful, but absolute. A prominent view in privilege law, advanced by Dean John Henry Wigmore[172] and repeatedly endorsed by the Supreme Court,[173] lower courts, and influential judges and commentators,[174] is that facially unqualified privileges offer absolute protection that cannot be overcome by any showing of a litigant's need for the information.[175] Imwinkelried has challenged that paradigm both descriptively and normatively. He argues that criminal defendants' Sixth Amendment rights,[176] and potentially civil litigants' Fifth and Fourteenth Amendment rights,[177] do and should qualify even purportedly absolute privileges when a litigant demonstrates sufficient need for privileged information.[178] From either viewpoint, privileges mark a legal zenith of information protection.

At the same time, privileges' remarkable power imposes well-recognized costs. The Supreme Court has repeatedly recognized that

---

169 For instance, federal criminal subpoenas are available solely for information that is "evidentiary" and "admissible," meaning they cannot reach privileged information. Bowman Dairy Co. v. United States, 341 U.S. 214, 221 (1951); *see* FED. R. CRIM. P. 17; United States v. Iozia, 13 F.R.D. 335, 338 (S.D.N.Y. 1952).

170 18 U.S.C. § 2517(4).

171 *See* McArthur, *supra* note 167, at 751.

172 Edward J. Imwinkelried, *Questioning the Behavioral Assumption Underlying Wigmorean Absolutism in the Law of Evidentiary Privileges*, 65 U. PITT. L. REV. 145, 147 (2004).

173 *See, e.g.*, Swidler & Berlin v. United States, 524 U.S. 399, 406 (1998); Jaffee v. Redmond, 518 U.S. 1, 9 (1996); Upjohn Co. v. United States, 449 U.S. 383, 393 (1981); *see also* Imwinkelried, *supra* note 172, at 148–49.

174 Imwinkelried, *supra* note 172, at 155–56; *see also* Richard A. Posner, *An Economic Approach to the Law of Evidence*, 51 STAN. L. REV. 1477, 1531 (1999).

175 Imwinkelried, *supra* note 172, at 147; *see also* Edward J. Imwinkelried, *The Dangerous Trend Blurring the Distinction Between a Reasonable Expectation of Confidentiality in Privilege Law and a Reasonable Expectation of Privacy in Fourth Amendment Jurisprudence*, 57 LOY. L. REV. 1, 8 (2011).

176 Imwinkelried, *supra* note 172, at 162–67.

177 *Id.* at 168–73.

178 *Id.* at 163. Privileges can also be facially qualified. *See, e.g.*, CAL. EVID. CODE § 1062(a) (West 2021).

"privileges impede the search for the truth."[179] At least in individual cases,[180] privileges are anti-accuracy, antitransparency, and harmful to litigants and the truth-seeking process.[181] Both lawyers and priests, for instance, have maintained the secrecy of privileged communications for decades, despite knowing that confidential information in their possession could exonerate innocent people serving lengthy sentences or even facing execution.[182] Parties denied access to privileged evidence may be ignorant of its existence and lack sufficient information to attempt proof by alternate means. In Professor Geoffrey Hazard Jr.'s compelling description, "the definition of [a] privilege will express a value choice between protection of privacy and discovery of truth and the choice of either involves the acceptance of an evil — betrayal of confidence or suppression of truth."[183]

Thus, when courts recognize a novel evidentiary privilege, whether by using their common law authority or by construing a statute as creating a privilege, they must accept the consequences of establishing a new, and potentially absolute, power to suppress relevant evidence at any and all stages of judicial proceedings.

*3. Confidentiality Without Privilege.* — Given privileges' breadth, power, and extraordinary costs, it should not be surprising that the class of communications that have been elevated to privileged status is quite small. At the same time, legal protections for sensitive information are not a privilege or bust proposition; there are other, more common and less costly, forms of protection. Specifically, not all privacy statutes that contain broad nondisclosure mandates create a privilege to block judicial process; some such statutes instead protect privacy by imposing

---

179 Pierce County. v. Guillen *ex rel.* Guillen, 537 U.S. 129, 144 (2003); *see* United States v. Nixon, 418 U.S. 683, 710 (1974).

180 Even under a Wigmorean utilitarian view that privileges impose no cost to truth-seeking over time because, without privilege, the protected communications would not be made in the first place, *see* Imwinkelried, *supra* note 172, at 148, recognizing privilege in any individual case suppresses evidence in that case.

181 Privileges are so anathema to factfinding that some theorists resist classifying them as Rules of Evidence at all. *See* Alex Stein, *The New Doctrinalism: Implications for Evidence Theory*, 163 U. PA. L. REV. 2085, 2094 n.47 (2015).

182 *See* Jim Dwyer, *In Court, a Priest Reveals a Secret He Carried for 12 Years*, N.Y. TIMES (July 17, 2001), https://www.nytimes.com/2001/07/17/nyregion/in-court-a-priest-reveals-a-secret-he-carried-for-12-years.html [https://perma.cc/PQX3-X2YF]; Adam Liptak, *When Law Prevents Righting a Wrong*, N.Y. TIMES (May 4, 2008), https://www.nytimes.com/2008/05/04/weekinreview/04liptak.html [https://perma.cc/GH3L-MAPL]. Some maintain that certain privileges should be absolute even in those extreme circumstances. *See* Swidler & Berlin v. United States, 524 U.S. 399, 410–11 (1998).

183 Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CALIF. L. REV. 1061, 1085 (1978).

*confidentiality* requirements.[184] Confidentiality requirements protect sensitive information in circumstances other than litigation but nonetheless yield to court orders and subpoenas. As the American Law Institute *Principles of the Law of Data Privacy* state in guidance for privacy legislation, "[a] duty of confidentiality is not breached . . . [whenever] disclosure is required by law, such as judicial process."[185]

Statutes that protect sensitive information through broad nondisclosure mandates, without blocking judicial process, reflect the well-established parameters of confidentiality law.[186] For instance, doctors have long owed their patients duties of confidentiality, yet medical records remain discoverable with valid judicial process.[187] Indeed, the FRE even make special provisions for the admissibility of patients' statements to their doctors, the rationale being that such statements have an extra guarantee of trustworthiness "in view of the patient's

---

184 For examples of statutes with broad confidentiality provisions that courts have construed to *not* create a privilege blocking judicial process, and instead to create mere confidentiality, see *Zambrano v. INS*, 972 F.2d 1122, 1125 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993); *United States v. Hernandez*, 913 F.2d 1506, 1151 (10th Cir. 1990); *In re Nelson*, 873 F.2d 1396, 1397 (11th Cir. 1989); *In re Nassau County Strip Search Cases*, No. 99-CV-2844, 2017 WL 3189870, at *5 (E.D.N.Y. July 26, 2017); *Rodriguez v. Robbins*, No. CV 07-3239, 2012 WL 12953870, at *2–3 (C.D. Cal. May 3, 2012); *Hassan v. United States*, No. C05-1066, 2006 WL 681038, at *3 (W.D. Wash. Mar. 15, 2006); *Seales v. Macomb County*, 226 F.R.D. 572, 576 (E.D. Mich. 2005); *Wilkins v. United States*, No. 99-CV-1579, 2004 U.S. Dist. LEXIS 29428, at *16–17 (S.D. Cal. 2004); *In re Grand Jury Subpoena Duces Tecum*, No. 101MC00005, 2001 WL 896479, at *4 (W.D. Va. June 12, 2001); *Schultz v. Talley*, 152 F.R.D. 181, 187 (W.D. Mo. 1993); *Van Emrik v. Chemung County Department of Social Services*, 121 F.R.D. 22, 25 (W.D.N.Y. 1988); *Bowman v. Consolidated Rail Corp.*, 110 F.R.D. 525, 527 (N.D. Ind. 1986); and *Merchants National Bank & Trust Co. of Fargo v. United States*, 41 F.R.D. 266, 268 (D.N.D. 1966). Thus, the bulk of federal statutes create "confidentiality rather than privilege," and even without an explicit exception for judicial process, "courts tend to construe . . . statutes as not creating a privilege." 23A GRAHAM & MURPHY, *supra* note 144, § 5437.

185 PRINCIPLES OF THE L., *supra* note 46, § 6(d).

186 *See generally* Richards & Solove, *supra* note 46.

187 *See* Jaffee v. Redmond, 518 U.S. 1, 10 (1996) (noting federal courts' rejection of a physician-patient privilege); Whalen v. Roe, 429 U.S. 589, 602 n.28 (1977) ("The physician-patient evidentiary privilege is unknown to the common law."); *In re* Zyprexa Prods. Liab. Litig., 254 F.R.D. 50, 53–54 (E.D.N.Y. 2008) (examining relationship between court-ordered disclosures and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of the U.S. Code)), *aff'd*, Nos. 04-MD-1596, 07-CV-645, 05-CV-01549, 05-CV-1455, 06-CV-5826, 07-CV-1749, 07-CV-1933, 08-CV-955, 2008 WL 4682311 (E.D.N.Y. Oct. 21, 2008); *see also* HIPAA Disclosure Rules, 45 C.F.R. § 164.512(e)(1)(ii)–(vi) (2019) (subpoena exception).

strong motivation to be truthful."[188] Attorneys owe duties of confidentiality to their clients,[189] but not all attorney work products are privileged.[190] The transcript of an attorney's interview with potential witnesses, for example, is subject to discovery in litigation.[191] Similarly, banks and accountants owe duties of confidentiality to their clients,[192] but they cannot withhold their clients' financial information from the courts.[193]

Of course, confidentiality and privilege share certain characteristics. Both reflect similar policy rationales that restricting disclosure of certain sensitive information will facilitate important relationships and communications.[194] They also have key differences. Confidentiality is more expansive than privilege, covering more substantive categories of information.[195] Privileges, in contrast, generally attach to highly specific categories of information; they often include a communicant's expectation of confidentiality as an element[196] and are limited by both the relationship of the communicants and the subject matter of the communication.[197] Confidentiality is also less costly to courts. Confidentiality may be enforceable through professional discipline or civil liability,[198] but unlike privilege it does not undermine the truth-seeking process of the judiciary.[199]

---

188 FED. R. EVID. 803(4) advisory committee's note; *see id.* 803(4). The rule against hearsay generally precludes admission of out-of-court statements introduced for the truth of the matter asserted, *see id.* 801–802, but a special exception allows a patient's out-of-court statement to a doctor for medical diagnosis or treatment to be admitted for its truth, *id.* 803(4).

189 *See* IMWINKELRIED, *supra* note 160, § 1.3.2.

190 *See, e.g.*, *In re* N.Y. Renu with Moistureloc Prod. Liab. Litig., Nos. 766,000/2007, MDL. 1785, C/A 06-MN-77777, 2009 WL 2842745, at *4 (D.S.C. July 6, 2009) ("[A] report is qualifiedly immune from discovery only if it was prepared *solely* in anticipation of litigation.").

191 *See* Richard W. Beckler, Frederick Robinson & Wendy Sue Morphew, *Protecting Defense Evidence from Prosecutorial Discovery*, 68 WASH. U. L.Q. 71, 81–86 (1990).

192 *See* IMWINKELRIED, *supra* note 160, § 1.3.1.

193 *See, e.g.*, 18 U.S.C. § 986; Trump v. Vance, 140 S. Ct. 2412, 2429–30 (2020) (acknowledging that a state criminal subpoena may compel an accounting firm to disclose a client's personal financial records); *see also* Young v. U.S. Dep't of Just., 882 F.2d 633, 641–43 (2d Cir. 1989) (explaining that banker-client duties of confidentiality do not create a testimonial privilege); Stokwitz v. United States, 831 F.2d 893, 894–97 (9th Cir. 1987).

194 *See Young*, 882 F.2d at 640–43 (generally comparing and contrasting tort of breach of confidence to the law of privilege).

195 Richards & Solove, *supra* note 46, at 135.

196 *See* 23A GRAHAM & MURPHY, *supra* note 144, § 5460 n.1.

197 The attorney-client privilege, for instance, applies solely to communications between a lawyer and a client, and solely to communications made in confidence in order to facilitate the provision of legal services. *See* PAUL F. ROTHSTEIN, FEDERAL TESTIMONIAL PRIVILEGES § 2:10 (2d ed.) (Westlaw) (last visited Apr. 10, 2021).

198 *See generally* PRINCIPLES OF THE L., *supra* note 46, § 1 ("The tort of breach of confidentiality protects against disclosures of confidential data made by doctors, lawyers, and others in a fiduciary relationship or an equivalent type of relationship.").

199 *See* IMWINKELRIED, *supra* note 160, § 1.3.7.

*4. The Current Stored Communications Act Privilege.* — In current case law, courts have construed SCA section 2702[200] to block criminal defense subpoenas for an ex ante category of relevant information: electronic communications contents possessed by technology companies.[201] Therefore, applying the definition of privilege induced above, courts have read the SCA as impliedly creating an unqualified evidentiary privilege.

There are three likely counterarguments to this position. These counterarguments are, roughly, *text*, *source*, and *admissibility*. The *admissibility* argument is the strongest challenge, but all three are ultimately unconvincing.

To start, one could take the position that the plain *text* of section 2702 does not use the word "privilege," so courts construing this statute must be creating something else entirely. But it is neither necessary nor sufficient for a statute to use the word "privilege" to create one. The Supreme Court has twice construed statutes that did not use the word as creating privilege.[202] Meanwhile, the Court of Federal Claims has

---

[200] Section 2702 states, in relevant part:

> Voluntary disclosure of customer communications or records
>
> (a) PROHIBITIONS. — Except as provided in subsection (b) or (c) —
>
> (1) 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; . . . .
>
> (b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS. — A provider described in subsection (a) may divulge the contents of a communication —
>
> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
>
> (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
>
> (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
>
> (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;
>
> (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (6) to the National Center for Missing and Exploited Children . . . ;
>
> (7) to a law enforcement agency . . . ; or
>
> (8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or
>
> (9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement . . . .

18 U.S.C. § 2702(a)–(b).

[201] *See* Petition for a Writ of Certiorari, *supra* note 7, at 11–13 (collecting criminal cases).

[202] *See* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 134, 145 (2003); Baldrige v. Shapiro, 455 U.S. 345, 354–55, 361 (1982); *see also Privilege*, *supra* note 159 (observing that the term "privilege" can be used generally to describe "the right to prevent disclosure of certain information in court").

held that a statute's use of the phrase "privileged proprietary information"[203] did not create a privilege because mere use of the term "privilege" "does not necessarily signify that Congress intended the information . . . to be immune from discovery."[204] In short, statutory privileges are defined not by what they are called but rather by what they do.

Nor does it matter that section 2702, as currently interpreted to block criminal defense subpoenas, restricts access to a particular *source* of evidence — namely providers of electronic communications services — rather than access to the underlying communications content itself.[205] Many privileges protect sources of information, not underlying facts. They protect certain statements made to certain people under certain conditions, without protecting the same statements communicated to, and sourced from, anyone else. The attorney-client privilege, for instance, protects some statements that a client makes to their attorney, but not the same statements obtained from the client's accountant or friend.[206] So too with statutory privileges; they may protect records obtained from a particular source but not those same records obtained elsewhere.[207] Topical privileges, such as those for trade secrets, state secrets, political votes, and informant's identity, are the exceptions that prove the rule. These privileges do shield underlying information, regardless of the source from which it was obtained.[208] But the fact that a statute shields one source of information and not another hardly excludes it from privilege status; source specificity merely edges the statute closer to the canonical relational privileges than the exceptional topical variety. Thus, even though courts have construed section 2702 to block judicial process for communications contents obtained from one source and not others, that fact does not refute the conclusion that this construction of the statute creates an evidentiary privilege.

---

[203] Jicarilla Apache Nation v. United States, 60 Fed. Cl. 611, 612 (2004) (quoting 25 U.S.C. § 2103(c)).

[204] *Id.*

[205] In some cases, criminal defendants might be able to subpoena the same protected content from an alternate source, such as the account holders or intended recipients of a communication, provided those alternate sources are accessible. *But cf. supra* p. 2741 (describing circumstances when these alternate routes are not accessible).

[206] *See* Upjohn Co. v. United States, 449 U.S. 383, 395–96 (1981).

[207] *See, e.g.*, Krizak v. W.C. Brooks & Sons, Inc., 320 F.2d 37, 43–44 (4th Cir. 1963) (construing a statute providing that an accident "report may not be used in evidence" to bar admission of the report itself, but not to bar the statements contained within the report, *id.* at 43); Sanborn v. Parker, No. 99 CV P678, 2005 WL 5190487, at *20–21, *23 (W.D. Ky. Jan. 12, 2005) (construing statutory attorney-client privilege to cover communications to an attorney but not communications made to an expert witness retained by the attorney), *modified*, No. 99-678, 2007 WL 495202 (W.D. Ky. Feb. 14, 2007), *rev'd in part on other grounds*, 629 F.3d 554 (6th Cir. 2010).

[208] *See* IMWINKELRIED, *supra* note 160, § 8.1.

The strongest — though ultimately unsuccessful — ground to try to distinguish the current consensus reading of section 2702 from a privilege is the view that the SCA shields information from judicial compulsory process, but does not separately shield the information from *admissibility* into evidence. Yet a distinct admissibility bar is, once again, neither necessary nor sufficient to satisfy the definition of a privilege. As a doctrinal matter, the Supreme Court has construed a statute that lacked a distinct admissibility bar as creating a privilege.[209] And an admissibility bar alone cannot distinguish privileges from the multitude of other evidence rules that block admissibility solely or primarily at trial, such as the rules on hearsay and character evidence.[210] Moreover, from a policy perspective, evidence that is inaccessible to judicial process is lost to the truth-seeking process of the courts as surely as is evidence that is inadmissible.[211] Just like the canonical common law privileges, the current SCA subpoena bar applies at every stage of a case, and blocks pretrial subpoenas, trial subpoenas, and live witness testimony from the stand.[212] And, of course, blocking live witness testimony simultaneously blocks the admission of that testimony into evidence. A distinct admissibility bar is thus a definitionally nonessential, if common, feature of privilege.

---

[209] In *Baldrige v. Shapiro*, the Court held that sections 8(b) and 9(a) of the Census Act, 13 U.S.C. §§ 8–9, created an evidentiary privilege, where the statutory text embodied "explicit congressional intent to preclude *all* disclosure of raw census data," Baldrige v. Shapiro, 455 U.S. 345, 361 (1982), and stated on its face that "[c]opies of census reports . . . shall be immune from legal process," 13 U.S.C. § 9(a); *see Baldrige*, 455 U.S. at 360–61, 360 n.16. The Court recognized the statute as creating a privilege despite the lack of any textual reference to admissibility as a separate and distinct issue from the general bar on legal process. *See Baldrige*, 455 U.S. at 360–61. Of course, some statutory privileges do provide express exclusionary rules alongside express bars on compulsory legal process. The statute at issue in *Pierce County v. Guillen ex rel. Guillen*, 537 U.S. 129 (2003), for instance, states that protected information "shall not be subject to discovery *or admitted into evidence*," *id.* at 135 (emphasis added) (quoting 23 U.S.C. § 409).

[210] *Cf.* 31 VICTOR J. GOLD, FEDERAL PRACTICE AND PROCEDURE § 8076(c) (1st ed.) (Westlaw) (last visited Apr. 10, 2021) ("The policy behind extending privilege law to all proceedings is that the values protected by privileges can be destroyed by permitting disclosure of privileged material in any judicial context.").

[211] The rules of access may in turn impact the rules of evidence. *See* Ronald J. Allen, *The Hearsay Rule as a Rule of Admission Revisited*, 84 FORDHAM L. REV. 1395, 1397 (2016) ("Rules of evidence have different implications in procedural regimes with and without cheap access to evidence."); *cf.* Maggie Wittlin, *Meta-evidence and Preliminary Injunctions*, 10 U.C. IRVINE L. REV. 1331, 1335 (2020) (identifying a useful category of "meta-evidence," or "evidence of what evidence will be produced at trial," and therefore paving the way to theorize information accessible to litigants and presented in pretrial proceedings *as a form of evidence* that raises similar policy concerns to evidence introduced at trial).

[212] *Compare* O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 86 (Ct. App. 2006) ("[The SCA] clearly prohibits any disclosure of [covered information] other than as authorized by enumerated exceptions."), *and* 18 U.S.C. § 2702(b) (containing no exception for defense legal process), *with* FED. R. EVID. 1101(c) ("The rules on privilege apply to all stages of a case or proceeding.").

A more nuanced articulation of the *admissibility* counterargument might rely on the fact that the SCA lacks a distinct suppression remedy for information obtained in violation of its statutory protections.[213] Yet, further scrutiny shows that it is also definitionally nonessential for a statutory privilege to suppress evidence obtained in violation of the statute's protections. Indeed, the canonical marital communications privilege also lacks an exclusionary rule for information obtained in violation of its privilege protections. Violations occur in at least two circumstances: via eavesdropping or through betrayal by the confidant.[214] The majority rule at common law and today is that the marital communications privilege lacks a distinct suppression remedy for communications overheard by a third-party eavesdropper, even when spouses take reasonable precautions to protect confidentiality.[215] And some courts also refuse to exclude communications where eavesdropping occurred because of the recipient-spouse's betrayal of confidence.[216] Thus, privileges sometimes lack exclusionary rules for evidence obtained by their violation.[217] The SCA's lack of a suppression remedy cannot remove current judicial constructions of the statute from the domain of privilege.

The following section examines the doctrinal consequences that flow from the observation that courts have read section 2702 as impliedly creating a privilege. Courts persuaded by the definitional argument advanced in this section should be bound by the doctrinal rules explained

---

[213] *See* 18 U.S.C. § 2707 (providing a private cause of action for injunctive relief, damages, and fees and costs); *id.* § 2708 (providing that the SCA's remedial provision is the exclusive remedy for SCA violations); *see also* United States v. Ferguson, 508 F. Supp. 2d 7, 10 (D.D.C. 2007) ("[T]he Stored Communications Act does *not* provide an exclusion remedy. It allows for civil damages . . . and criminal punishment . . . but nothing more." (quoting United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998) (citations omitted))). In contrast, statutory privileges that do contain distinct admissibility bars alongside express bars on compulsory legal process have the effect of providing such a suppression remedy. The statute at issue in *Pierce*, for instance, not only bars legal process but also suppresses evidence obtained in violation of that bar. *See supra* note 209.

[214] *See* IMWINKELRIED, *supra* note 160, § 6.6.5.

[215] *See generally* JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE § 2339 & n.1 (4th ed. Supp. 2021) (Wolters Kluwer) (last accessed Apr. 10, 2021). The rule may be somewhat different for the attorney-client privilege. When violations of the attorney-client privilege occur through unlawful computer hacking, courts are split as to whether the privilege is destroyed or affords a suppression remedy; the answer may turn on whether the privilege holder took reasonable cybersecurity precautions to protect the information, but the doctrine is still evolving. *See* ROTHSTEIN, *supra* note 197, § 2:16. *See generally* Anne E. Conroy, *Reevaluating Attorney-Client Privilege in the Age of Hackers*, 82 BROOK. L. REV. 1817, 1824–25 (2017).

[216] *See, e.g.*, United States v. Neal, 532 F. Supp. 942, 948–49 & nn.6–7 (D. Colo. 1982) (collecting cases that are split on this issue), *aff'd*, 743 F.2d 1441 (10th Cir. 1984).

[217] *See* ROTHSTEIN, *supra* note 197, § 1:1; United States v. Haynes, 216 F.3d 789, 802 (9th Cir. 2000). Note that when the privilege at issue is a "professional" privilege (for example, attorney-client, priest-penitent), courts "almost uniformly" permit the privilege holder to exclude evidence obtained through breach by the confidant. IMWINKELRIED, *supra* note 160, § 6.6.5.

below. If, in the alternative, current judicial readings of section 2702 are merely analogous to privilege, the policies underlying the doctrinal rules — namely, the mandate to prioritize the truth-seeking process of the judiciary — should counsel a similar result.

### *B. The Rules that Govern Statutory Privilege Construction*

This section offers a novel analysis of Supreme Court and appellate doctrine that controls when courts must, and must not, construe federal statutes to block judicial process and create privilege. It contends that courts should not construe a federal statute to block judicial process unless the plain text of the statute clearly indicates congressional intent to create an evidentiary privilege. In the process, it also identifies a previously unrecognized federal circuit split as to whether, or in what circumstances, courts may construe ambiguous silence in statutory text as impliedly creating a privilege. The Ninth, Tenth, and Eleventh Circuits have prioritized Congress's legislated subpoena and discovery rules that safeguard the truth-seeking process of the courts, and ruled that courts must not construe a federal statute as creating a privilege unless the statutory text expressly exempts information from judicial compulsory process.[218] The District of Columbia, Third, and Fifth Circuits have taken the contrary position that, in certain narrow circumstances, courts may construe ambiguous silence in statutory text as impliedly creating a privilege.[219] The split is ripe for Supreme Court review.

After analyzing this doctrine, this section applies it to the SCA. It argues that current SCA case law is inconsistent with Supreme Court doctrine and both sides of the federal circuit split on implied statutory privileges. Judges have improperly construed ambiguous silence in the text of section 2702 as impliedly creating a privilege, despite a reasonable nonprivilege reading that the text creates mere confidentiality. In doing so, judges have facilely attributed to Congress what is a vast and unprecedented new privilege for the internet.

*1. The Strict Construction Rule.* — Courts, lawmakers, and commentators have long expressed concern that privileges could balloon unwisely, to the detriment of the truth-seeking process of adjudication.[220] One key limit buffering against this risk is the *narrow construction* mandate. The Supreme Court has held repeatedly that federal courts must

---

[218] *See* Zambrano v. INS, 972 F.2d 1122, 1125–26 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993); United States v. Hernandez, 913 F.2d 1506, 1511–12 (10th Cir. 1990); *In re* Nelson, 873 F.2d 1396, 1397 (11th Cir. 1989).

[219] *See* Cazorla v. Koch Foods of Miss., L.L.C., 838 F.3d 540, 552 (5th Cir. 2016); *In re* England, 375 F.3d 1169, 1177 (D.C. Cir. 2004); Pearson v. Miller, 211 F.3d 57, 68 (3d Cir. 2000).

[220] *See supra* pp. 2749–50.

construe privileges narrowly because of their extraordinary cost to judicial truth-seeking.[221] Perhaps the most influential formulation of this rule was the Supreme Court's statement in *United States v. Nixon*, "privileges against forced disclosure [are] established in the Constitution, by statute, or at common law. Whatever their origins, these exceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth."[222] This principle has been so long ingrained in law that Wigmore, writing in 1905, observed that "[f]or three hundred years it has now been recognized as a fundamental maxim that the public . . . has a right to every man's evidence"[223] and "all privileges of exemption from this duty are exceptional, and are therefore to be discountenanced."[224]

Accordingly, when federal courts exercise common law authority to create new evidentiary privileges "in the light of reason and experience,"[225] they begin with a presumption that "there is a general duty to give what testimony one is capable of giving."[226] Courts then must conduct a careful balancing analysis to determine whether a proposed privilege "promotes sufficiently important interests to outweigh the need for probative evidence in the administration of criminal justice."[227]

For statutory privileges, the overarching presumption in favor of truth-seeking and against privilege remains, but the analysis somewhat differs. Courts should, of course, begin with the text. Privacy and confidentiality provisions in statutory text fall into three groups: those that expressly privilege or exempt information from judicial process,[228] those that expressly subject information to judicial process,[229] and those that are silent on disclosures pursuant to judicial process.[230] The existence of the two express categories demonstrates that Congress knows how to

---

[221] *See, e.g.*, United States v. Nixon, 418 U.S. 683, 710 (1974). Most, if not all, states have analogous rules. *See, e.g.*, *In re* Storror, 63 F. 564, 566–67 (N.D. Cal. 1894). *Cf. generally* Abbe R. Gluck & Lisa Schultz Bressman, *Statutory Interpretation from the Inside — An Empirical Study of Congressional Drafting, Delegation, and the Canons: Part I*, 65 STAN. L. REV. 901 (2013).

[222] *Nixon*, 418 U.S. at 709–10; *see also* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 144 (2003) ("[S]tatutes establishing evidentiary privileges must be construed narrowly . . . .").

[223] 4 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2192, at 2965 (1905). More recently, the Supreme Court credited the maxim that "the public has a right to every man's evidence" to a 1742 English parliamentary debate. Trump v. Vance, 140 S. Ct. 2412, 2420 (2020); *see id.* at 2420 n.1 (citing 12 THE PARLIAMENTARY HISTORY OF ENGLAND 693 (1812)).

[224] 4 WIGMORE, *supra* note 223, § 2192, at 2968.

[225] FED. R. EVID. 501.

[226] Jaffee v. Redmond, 518 U.S. 1, 9 (1996).

[227] Trammel v. United States, 445 U.S. 40, 51 (1980); *see also Jaffee*, 518 U.S. at 9–10 (quoting *Trammel*, 445 U.S. at 51).

[228] *See, e.g.*, 13 U.S.C. § 9(a).

[229] *Cf., e.g.*, 45 C.F.R. § 164.512(e)(1)(vi) (2019).

[230] *See, e.g.*, 8 U.S.C. § 1255a(c)(5)(A)(i)–(iii).

create, and preclude, evidentiary privileges when it wants to do so.[231] In contrast, statutes that are silent on disclosures pursuant to judicial process are ambiguous as to their effect on judicial process.[232]

When faced with the task of construing such ambiguous statutes, courts do not conduct the balancing of competing interests required to recognize novel common law privileges. Instead, courts assessing purported statutory privileges must determine whether the statute abrogates the legislatively crafted subpoena, discovery, and evidence rules, or merely imposes a confidentiality requirement that yields to court orders.[233] Put another way, construing a statute as creating privilege, rather than mere confidentiality, means construing that statute to supersede the procedural rules that have been promulgated by the Judicial Conference of the United States and approved by the United States Supreme Court, prior to review by Congress pursuant to the Rules Enabling Act.[234]

In this context, the general narrow construction mandate for all evidentiary privileges translates into a strict construction rule for statutory privileges in particular.[235] Judge Weinstein's leading treatise on evi-

---

[231] Note that some courts have interpreted even the express privilege category as remarkably narrow. The Supreme Court has clarified that statutory language expressly immunizing information from legal process can suffice to create an evidentiary privilege. *See* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 135, 145 (2003). But, due to the strong presumption against construing federal statutes to create evidentiary privilege, some courts have held that even the use of the word "privilege" in statutory text is not always sufficient to create a privilege that blocks court-ordered legal process. *See* Jicarilla Apache Nation v. United States, 60 Fed. Cl. 611, 612 (2004).

[232] *Cf.* United States v. Hernandez, 913 F.2d 1506, 1511 (10th Cir. 1990) (observing that language in the Immigration Reform and Control Act of 1986 (IRCA), Pub. L. No. 99-603, 100 Stat. 3359 (codified in scattered sections of the U.S. Code), that prohibits the "use," "publication," and "examin[ation]" of information, *Hernandez*, 913 F.2d at 1511 (quoting 8 U.S.C. § 1255a(c)(5)(A)), without mentioning privilege or judicial process, "is somewhat ambiguous as to the scope of the confidentiality requirement," *id.*).

[233] *See, e.g.*, Pearson v. Miller, 211 F.3d 57, 68 (3d Cir. 2000) ("Statutory provisions providing for duties of confidentiality do not automatically imply the creation of evidentiary privileges binding on courts."); Nguyen Da Yen v. Kissinger, 528 F.2d 1194, 1205 (9th Cir. 1975) ("The records are confidential but not privileged."). For additional examples of courts construing broad confidentiality provisions in statutory text as *not* creating a privilege to block judicial process, see *supra* note 184. *See generally* IMWINKELRIED, *supra* note 160, § 1.3.7 ("In some cases, a rule, especially a statutory one, generally limits the disclosure of certain types of information without [expressly] restricting disclosure during litigation. These rules do not create true privileges. . . . In many cases, though, the restriction has been construed as being limited to extrajudicial disclosure.").

[234] 28 U.S.C. § 2072. For an overview of the rulemaking process for the Federal Rules of Practice and Procedure, see *How the Rulemaking Process Works: Overview for the Bench, Bar, and Public*, U.S. CTS., https://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works/overview-bench-bar-and-public [https://perma.cc/6L5W-ZUYJ].

[235] *See, e.g.*, Univ. of Pa. v. EEOC, 493 U.S. 182, 189 (1990) ("[A]ny such privilege must 'be strictly construed.'" (quoting Trammel v. United States, 445 U.S. 40, 50 (1980))); Baldrige v. Shapiro,

dence law explains the rule as follows: "statutes asserted to create privileges should be construed strictly, so as to avoid suppressing otherwise competent evidence unless *no other conclusion* can be drawn from the statutory language."[236] To emphasize, there is no judicial discretion on this issue; courts are prohibited from construing a statute as creating privilege unless there is no reasonable alternative reading of the statutory text.[237]

The Supreme Court announced the strict construction rule in *St. Regis Paper Co. v. United States*.[238] The Court held that courts considering whether a federal statute creates an evidentiary privilege have a "duty to avoid a construction that would suppress otherwise competent evidence unless the statute, strictly construed, *requires such a result*."[239] *St. Regis* concerned an antitrust investigation in which the Federal Trade Commission subpoenaed the St. Regis Paper Company for copies of reports that the company had provided to the Census Bureau.[240] The company argued that section 9(a) of the Census Act[241] entitled it to not comply with the subpoena.[242] The Court disagreed.[243] At the time, section 9(a) contained a broad confidentiality provision that generally barred the Department of Commerce from "use," "publication," and "permit[ing] anyone . . . to examine" census reports.[244] Section 8

---

455 U.S. 345, 360 (1982) ("A statute granting a privilege is to be strictly construed . . . ."); *Trammel*, 445 U.S. at 50 (noting that privileges "must be strictly construed").

236 3 WEINSTEIN & BERGER, *supra* note 162, § 502A.05(1) (emphasis added).

237 *See* St. Regis Paper Co. v. United States, 368 U.S. 208, 218 (1961).

238 368 U.S. 208.

239 *Id.* at 218 (emphasis added); *see also* Robert G. Nath, *Internal Revenue Service Summonses for "Sensitive" Accountants' Papers*, 34 VAND. L. REV. 1561, 1592 (1981) ("*St. Regis Paper Co.* appears to resolve the competing policies in favor of disclosure, even though the Supreme Court assumed that the undesirable chilling effect would in fact occur.").

240 *St. Regis*, 368 U.S. at 213–15.

241 13 U.S.C. § 9.

242 *St. Regis*, 368 U.S. at 215. The Solicitor General, along with the Department of Commerce, the Census Bureau, and the Bureau of the Budget, agreed with the St. Regis company, arguing that section 9(a) rendered the copies of the reports "not subject to legal process," and "not subject to compulsive production." *Id.* at 217. The Federal Trade Commission and the Antitrust Division of the Department of Justice argued the opposite. *Id.*

243 *Id.* at 217.

244 At the time of *St. Regis*, section 9(a) of the Census Act stated *in full*:

> Information as confidential; exception.
>
> (a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, may, except as provided in section 8 of this title —
>
> (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or
>
> (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or
>
> (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports.

*Id.* at 216 n.5 (quoting 13 U.S.C. § 9(a) (1958) (current version at 13 U.S.C. § 9(a))).

enumerated a series of express exceptions permitting disclosure of limited categories of raw census data for certain purposes but remained facially silent as to disclosures pursuant to judicial process.[245] The Court concluded that section 9(a)'s "prohibitions" did not shield information possessed by the St. Regis Paper Company.[246] It based this conclusion squarely on the strict construction rule, explaining its holding as follows:

> Ours is the duty to avoid a construction that would suppress otherwise competent evidence unless the statute, strictly construed, requires such a result. That this statute does not do. . . . Indeed, when Congress has intended like reports not to be subject to compulsory process it has said so.[247]

To illustrate the conclusion that, "when Congress has intended like reports not to be subject to compulsory process it has said so," the Court pointed to two statutes that both contained express privilege language.[248]

The *St. Regis* holding did little new.[249] It merely reiterated for the statutory domain the well-established mandate that privileges must be

---

[245] 13 U.S.C. § 8 (1958) (current version at 13 U.S.C. § 8). The St. Regis company also claimed confidentiality protections from section 8, which, at the time, stated in relevant part:

> Certified copies of certain returns; other data; restriction on use; disposition of fees received.
>
> (a) The Secretary [of Commerce] may, upon a written request, and in his discretion, furnish to Governors of States and Territories, courts of record, and individuals, data for genealogical and other proper purposes, from the population, agriculture, and housing schedules prepared under the authority of subchapter II of chapter 5, upon the payment of the actual, or estimated cost of searching the records and $1 for supplying a certificate.
>
> (b) The Secretary may furnish transcripts or copies of tables and other census records and make special statistical compilations and surveys for State or local officials, private concerns, or individuals upon the payment of the actual, or estimated cost of such work. . . .
>
> (c) In no case shall information furnished under the authority of this section be used to the detriment of the persons to whom such information relates.

*Id.*; *see St. Regis*, 368 U.S. at 215. The Court ruled that section 8 was wholly inapplicable to the facts of *St. Regis*. *St. Regis*, 368 U.S. at 215.

[246] *St. Regis*, 368 U.S. at 217; *see id.* at 217–18 (holding that "the prohibitions against disclosure contained in § 9 run only against the officials receiving such information," *id.* at 217, without commenting — even in passing dicta — on the scope of those section 9(a) "prohibitions" in hypothetical circumstances where they might, counterfactually, have applied).

[247] *Id.* at 218.

[248] *Id.* One statute stated that "neither said report . . . nor any part thereof shall be admitted as evidence or used for any purpose in any suit or action for damages," *id.* at 218 n.8 (quoting Act of May 6, 1910, ch. 208, § 4, 36 Stat. 351 (repealed 1994)), and the other stated that "no report . . . shall be admitted as evidence, or used for any other purpose, in any suit or action for damages," *id.* at 218 n.9 (quoting 49 U.S.C. § 320(f) (1958) (current version at 49 U.S.C. § 504(f))).

[249] Importantly, the Court in *St. Regis* did not decide whether the broad confidentiality protections in section 9(a)'s plain text created a statutory privilege for information possessed by the Department of Commerce. *See St. Regis*, 368 U.S. at 215 ("[T]he Commission [has] not been furnished any information by the Secretary [of Commerce] . . . ."); *cf.* Pierre N. Leval, *Judging Under the Constitution: Dicta About Dicta*, 81 N.Y.U. L. REV. 1249, 1277–78 (2006). To the contrary, the opinion scrupulously avoided language that might be read to characterize those protections as an evidentiary privilege, even in passing dicta. Instead, the Court's description tracked the language

construed narrowly because they suppress relevant evidence from the truth-seeking process of the judiciary. In the years following *St. Regis*, the Court has repeatedly reasserted the narrow construction mandate for privileges in general,[250] and the strict construction rule for statutory privileges in particular.[251]

*2. Express Statutory Privileges.* — There are only two conceivable circumstances in which no plausible reading of a statute exists other than as creating a privilege: either the text expressly indicates congressional intent to create a privilege, or it does so by implication. The Ninth, Tenth, and Eleventh Circuits have held that federal statutes must

---

of the statute itself, characterizing the prohibitions as "restrictions," *St. Regis*, 368 U.S. at 218, on "us[e]," *id.* at 215, "publication," *id.* at 216, and permission "to examine" protected information, *id.* (quoting 13 U.S.C. § 9(a) (1958)), without referencing privilege or judicial process, *see id.* at 215–16. This is so despite the fact that the Solicitor General argued that section 9(a) created a privilege, *see* Brief for the United States at 29, 49, *St. Regis*, 368 U.S. 215 (No. 47), and despite the fact that the *St. Regis* opinion acknowledged the Solicitor General's view immediately before rejecting it, *see* 368 U.S. at 218.

Moreover, the fact that the Court illustrated its conclusion that "when Congress has intended like reports not to be subject to compulsory process it has said so" by pointing to two express privilege statutes, and not to section 9(a), indicates that the Court may *not* have believed that section 9(a) protections created a statutory privilege, even for information possessed by the Department of Commerce. The citations support the view that statutory text expressly immunizing information from judicial process suffices to create privilege, but shed little light on the unresolved scope of section 9(a) protections.

Indeed, more than two decades would pass before the Court would address whether section 9(a) created an evidentiary privilege. *See* Baldrige v. Shapiro, 455 U.S. 345, 362 (1982); *infra* p. 2768. In the interim, the lower courts would split on the issue. *See* Carey v. Klutznick, 653 F.2d 732, 739 (2d Cir. 1981) (stating that the Third and Tenth Circuits were split on this issue, then embracing the Tenth Circuit view). Some lower courts that did recognize a privilege for information possessed by the Census Bureau during the interim period between *St. Regis* and *Baldrige* did so not by relying on either *St. Regis*'s holding or the plain text of section 9(a), but rather by using their common law authority to conduct the careful balancing required before courts may recognize new common law privileges. *See, e.g.*, United States v. Int'l Bus. Machs. Corp., 20 Fed. R. Serv. 2d 1082, 1086–88 (S.D.N.Y. 1975) ( "The court's decision about whether to allow or reject the claim of privilege [concerning census data] must be based on a balancing of competing policies." *Id.* at 1087.).

[250] *See, e.g.*, Baker v. Gen. Motors Corp., 522 U.S. 222, 239 (1998); Swidler & Berlin v. United States, 524 U.S. 399, 411 (1998) (O'Connor, J., dissenting); Jaffee v. Redmond, 518 U.S. 1, 19 (1996) (Scalia, J., dissenting); Univ. of Pa. v. EEOC, 493 U.S. 182, 189 (1990); Trammel v. United States, 445 U.S. 40, 50 (1980); Herbert v. Lando, 441 U.S. 153, 175 & n.24 (1979); United States v. Nixon, 418 U.S. 683, 710 (1974); Branzburg v. Hayes, 408 U.S. 665, 690 n.29 (1972) (citing Wigmore, Professor Edmund Morgan, Professor Charles McCormick, Judge Learned Hand, and others in accord); Elkins v. United States, 364 U.S. 206, 234 (1960) (Frankfurter, J., dissenting).

[251] *See* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 144–45 (2003) ("[T]o the extent the text of the statute permits, we must construe it narrowly." *Id.* at 145.); *see also Baldrige*, 455 U.S. at 360.

contain express privilege language before courts may construe the statutes as blocking judicial process,[252] and a series of federal district courts have adopted similar reasoning and conclusions.[253]

There are strong grounds supporting this position. To start, Congress knows how to write an express statutory privilege when it wants to.[254] For instance, months after the *St. Regis* opinion, Congress amended section 9(a) of the Census Act to add the following language:

> Copies of census reports which have been so retained *shall be immune from legal process*, and shall not, without the consent of the individual or establishment concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.[255]

The amended Census Act joined a plethora of similarly worded companions. Communications to a "neutral" under the Administrative Dispute Resolution Act are not subject to "discovery or compulsory process."[256] Certain transportation reports "shall not be subject to

---

[252] Zambrano v. INS, 972 F.2d 1122, 1125 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993); United States v. Hernandez, 913 F.2d 1506, 1511 (10th Cir. 1990); *In re* Nelson, 873 F.2d 1396, 1397 (11th Cir. 1989).

[253] *See In re* Nassau Cnty. Strip Search Cases, No. 99-CV-2844, 2017 WL 3189870, at *6 (E.D.N.Y. July 26, 2017) (holding that federal statutes did not create a privilege to shield information from discovery because none "specifically provide[d] that information [was] not subject to discovery"); Chaplaincy of Full Gospel Churches v. England, 234 F.R.D. 7, 12 (D.D.C. 2006) (observing "the well established requirement that statutory bars to discovery be made expressly"); Hassan v. United States, No. C05-1066C, 2006 WL 681038, at *2 (W.D. Wash. Mar. 15, 2006) ("[S]tatutes prohibiting general disclosure of information do not bar judicial discovery absent an express prohibition against such disclosure." (citing *Zambrano*, 972 F.2d at 1125)); Wilkins v. United States, No. 99-CV-1579, 2004 U.S. Dist. LEXIS 29428, at *16 (S.D. Cal. Dec. 23, 2004) ("[T]he Ninth Circuit has stated that unless a statute contains specific language barring discovery in the judicial process, it will be narrowly construed to allow limited use of the protected information." (citing *Zambrano*, 972 F.2d at 1125)); Jicarilla Apache Nation v. United States, 60 Fed. Cl. 611, 612 (2004) (construing the phrase "privileged proprietary information" in statutory text as not creating privilege, relying on *Zambrano v. INS*, 972 F.2d 1122, and reasoning that mere use of the term "privilege" in the statute "neither specifically defines that rule or protection nor, especially, indicates that the protection extends to preventing disclosure by way of discovery"); *In re* Grand Jury Subpoena Duces Tecum, No. 101MC00005, 2001 WL 896479, at *2 (W.D. Va. June 12, 2001) ("[T]he Supreme Court has held that statutes prohibiting general disclosure of information do not bar judicial discovery absent an express prohibition against such disclosure." (citing *St. Regis*, 368 U.S. at 218)); *see also* 23A GRAHAM & MURPHY, *supra* note 144, § 5437 (noting that the bulk of federal statutes create "confidentiality rather than privilege," and that even without an explicit exception for judicial subpoenas, "courts tend to construe the statutes as not creating a privilege").

[254] *See Jicarilla*, 60 Fed. Cl. at 613 & n.1 (collecting statutes).

[255] Act of Oct. 15, 1962, Pub. L. No. 87-813, 76 Stat. 922 (codified at 13 U.S.C. § 9(a)) (emphasis added). A little over a decade later, Congress also amended section 8 to permit census information to be used "in the prosecution of alleged violations of [the Census Act]." Act of Oct. 17, 1976, Pub. L. No. 94-521, § 6(a), 90 Stat. 2460 (codified at 13 U.S.C. § 8). Despite these revisions, the rule announced in *St. Regis*, that courts have a "duty to avoid a construction that would suppress otherwise competent evidence unless the statute, strictly construed, requires such a result," *St. Regis*, 368 U.S. at 218, remains good law today, *see* 3 WEINSTEIN & BERGER, *supra* note 162, § 502A.05(1) & n.4 ("The *St. Regis* case remains authoritative . . . .").

[256] 5 U.S.C. § 574(a).

discovery,"[257] while others are "immune from legal process."[258] Federal highway aid information "shall not be subject to discovery."[259] Some foreign investment information "shall be immune from legal process."[260] Medicare and Medicaid data are "not . . . subject to discovery."[261] Some "patient safety work product" is " not . . . subject to discovery,"[262] while other consumer product safety reports "shall be immune from legal process and shall not be subject to subpoena or other discovery."[263] Certain audit materials are "privileged as an evidentiary matter."[264] "[T]he Firearms Trace System database . . . shall be immune from legal process . . . ."[265] Information obtained by the State Justice Institute "shall be immune from legal process."[266] The deliberations of military selection boards "are immune from legal process."[267] Communications between taxpayers and federally authorized tax practitioners are protected "to the extent the communication would be considered a privileged communication if it were between a taxpayer and an attorney."[268]

The fact that Congress chose not to include similar express language in other privacy and confidentiality statutes is a powerful sign that Congress did not intend those statutes to create a privilege exempting information from judicial compulsory process. The Supreme Court has repeatedly relied on this logic in other contexts. It recently admonished:

> Congress knows how to impose express limits on the availability of attorney's fees in ERISA cases. Because Congress failed to include in [29 U.S.C.] § 1132(g)(1) an express "prevailing party" limit on the availability of attorney's fees, the Court of Appeals' decision adding that term of art to a fee-

---

257 23 U.S.C. § 409; *see also* Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 145–46 (2003).

258 49 U.S.C. § 6307(b)(2)(B)(i)–(ii).

259 23 U.S.C. § 148(h)(4).

260 22 U.S.C. § 3144(d).

261 42 U.S.C. § 1395kk(e)(4)(D).

262 42 U.S.C. § 299b-22(a).

263 15 U.S.C. § 2055(e)(2).

264 15 U.S.C. § 7215(b)(5)(A).

265 Consolidated Appropriations Act, 2005 (Tiahrt Amendment), Pub. L. No. 108-447, 118 Stat. 2809, 2859 (2004) (codified at 18 U.S.C. § 923).

266 42 U.S.C. § 10708(b). "Immune from legal process" is a common textual formulation. *See* 20 U.S.C. § 9573(d)(1)(B) ("Individually identifiable [educational statistics] shall be immune from legal process and shall not . . . be admitted as evidence . . . ."); 34 U.S.C. § 10231(a) ("[Certain Office of Justice] information . . . shall be immune from legal process, and shall not . . . be admitted as evidence . . . ."); 34 U.S.C. § 20110(d) ("[Information concerning disbursements of the Crime Victims Fund] shall be immune from legal process and shall not . . . be admitted as evidence . . . ."); 49 U.S.C. § 6307(b)(2)(B)(i)–(ii) ("[Certain reports made to the Bureau of Transportation] shall be immune from legal process; and shall not . . . be admitted as evidence . . . .").

267 10 U.S.C. 613a(b).

268 26 U.S.C. § 7525(a). Thank you to Professor Daniel Capra for pointing out this taxpayer example of statutory language expressly creating privilege.

> shifting statute from which it is conspicuously absent more closely resembles "invent[ing] a statute rather than interpret[ing] one."[269]

The same reasoning applies to purported statutory privileges.

Supreme Court doctrine also supports — and perhaps requires — a rule that statutory privileges must be express. The Court has weighed in on statutory privileges at least thrice.[270] The most recent case in the trilogy, *Pierce County v. Guillen ex rel. Guillen*,[271] does not disprove the alternate view that statutory language may create privileges by implication, but it is consistent with a requirement that statutory privileges must be express. In *Pierce*, the Court construed a statute as creating a privilege where the plain text expressly shielded information from both pretrial discovery and admissibility in court.[272] The case concerned a federal statute requiring states to survey "hazardous locations" on their roads in order to qualify for federal aid to repair the roads.[273] Commentators expressed concerns that this survey requirement could subject states to increased liability for motor vehicle accidents, which might, in turn, discourage their "forthcoming and thorough" data collection.[274] Congress amended the statute to try to address those concerns. It first adopted a provision providing that, "[n]otwithstanding any other provision of law," data compiled for purposes of compliance with the road repair program "shall not be admitted into evidence in Federal or State court."[275] While that text clearly barred admissibility, some state courts continued to construe the statute to permit pretrial discovery.[276] A subsequent amendment added that the data was not "subject to discovery."[277] In 1995, Congress broadened the statute's reach once

---

[269] Hardt v. Reliance Standard Life Ins. Co., 560 U.S. 242, 252 (2010) (quoting Pasquantino v. United States, 544 U.S. 349, 359 (2005)); *see also* Meghrig v. KFC W., Inc., 516 U.S. 479, 485 (1996) ("Congress thus demonstrated in [the Comprehensive Environmental Response, Compensation, and Liability Act] that it knew how to provide for the recovery of cleanup costs, and that the language used to define the remedies under [the Resource Conservation and Recovery Act] does not provide that remedy."). Thank you to Professor Jonathan Gould for pointing me to these cases.

Admittedly, this argument could also cut the other way because statutes also exist that expressly subject information to compulsory legal process. *See* Ass'n for Women in Sci. v. Califano, 566 F.2d 339, 346 (D.C. Cir. 1977) (identifying three categories of statutes: express creation of privilege, express preclusion of privilege, and silence as to legal process); *see also* 3 WEINSTEIN & BERGER, *supra* note 162, § 502A.04(2)(c).

[270] Pierce County v. Guillen *ex rel.* Guillen, 537 U.S. 129, 132–33 (2003); Baldrige v. Shapiro, 455 U.S. 345, 347 (1982); St. Regis Paper Co. v. United States, 368 U.S. 208, 212 (1961).

[271] 537 U.S. 129.

[272] *Id.* at 135–36, 145; *see also St. Regis*, 368 U.S. at 218 ("[W]hen Congress has intended . . . reports not to be subject to compulsory process it has said so.").

[273] *Pierce*, 537 U.S. at 133 (quoting 23 U.S.C. § 152(a)).

[274] *Id.* at 134; *see id.* at 133–34.

[275] Surface Transportation and Uniform Relocation Assistance Act of 1987, Pub. L. No. 100-17, § 132, 101 Stat. 132, 170 (codified as amended at 23 U.S.C. § 409).

[276] *Pierce*, 537 U.S. at 134–35.

[277] Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, § 1035, 105 Stat. 1914, 1978 (codified as amended at 23 U.S.C. § 409).

again, by specifying that it applied to data that was either "collected" or "compiled."[278] *Pierce* held that this twice-amended statute "establishes a privilege."[279] While the case does not clarify whether such express language is necessary to create a privilege, it establishes that a statute stating that information "shall not be subject to discovery"[280] and "shall not be . . . admitted into evidence"[281] suffices to create a privilege.

Ultimately, the view that statutory privileges must be express goes back to the first of the trilogy, *St. Regis Paper Co. v. United States*. In *Zambrano v. INS*,[282] the Ninth Circuit cited *St. Regis* for its conclusion that "[t]he Supreme Court has held that statutes prohibiting general disclosure of information do not bar judicial discovery absent an express prohibition against such disclosure."[283] Recall that, in *St. Regis*, the Court announced the strict construction rule and concluded that statutory language that generally restricted the Department of Commerce from "use," "publication," or "permit[ting] anyone . . . to examine" raw census data, but that did not expressly exempt information from judicial process, did not create a privilege.[284] Recall as well that the Court cited two express statutory privileges to illustrate the observation that "when Congress has intended like reports not to be subject to compulsory process it has said so."[285] Similarly, in *Zambrano*, the Ninth Circuit held that a broad nondisclosure mandate in the Immigration Reform and Control Act of 1986[286] (IRCA) did not create a privilege.[287] The pertinent provision of the IRCA generally bars the possessor of covered information from "use," "publication," or "permit[ting] anyone . . . to examine" that information.[288] The statute then enumerates a series of express exceptions for permissible disclosures,[289] but is facially silent as to privilege, subpoenas, discovery orders, and judicial process.[290] The Ninth Circuit held that, because the IRCA's nondisclosure mandate

---

[278] National Highway System Designation Act of 1995, Pub. L. No. 104-59, § 323, 109 Stat. 568, 591 (codified as amended at 23 U.S.C. § 409).

[279] *Pierce*, 537 U.S. at 145.

[280] 23 U.S.C. § 409.

[281] *Id.*

[282] 972 F.2d 1122 (9th Cir. 1992), *vacated and remanded on other grounds,* 509 U.S. 918 (1993).

[283] *Id.* at 1125 (citing St. Regis Paper Co. v. United States, 368 U.S. 208 (1961)).

[284] *St. Regis*, 368 U.S. at 216 n.5 (quoting 13 U.S.C. § 9(a) (1958) (current version at 13 U.S.C. § 9(a))); *see id.* at 218.

[285] *See id.* at 218; *see also supra* notes 238–248 and accompanying text.

[286] Pub. L. No. 99-603, 100 Stat. 3359 (codified in scattered sections of the U.S. Code).

[287] *Zambrano*, 972 F.2d at 1125–26.

[288] 8 U.S.C. § 1255a(c)(5)(A)(i)–(iii).

[289] *See id.* § 1255a(c)(5)(B)–(C) (permitting disclosures to law enforcement, to medical coroners, and in "circumstances as census information may be disclosed by the Secretary of Commerce under section 8 of title 13," *id.* § 1255a(c)(5)(C)).

[290] *Id.* § 1255a(c)(5)(A)(i)–(iii).

"d[id] not specifically prohibit judicial disclosure,"[291] it was "not violated by . . . court ordered discovery."[292]

Though somewhat less sweeping in its language, the Eleventh Circuit similarly relied on *St. Regis* to hold that statutory nondisclosure provisions that do not expressly immunize information from legal process do not privilege that information from compelled production in discovery.[293] In *In re Nelson*,[294] the Eleventh Circuit construed another section of the IRCA that contains identical statutory text to that at issue in *Zambrano*.[295] *In re Nelson* held that this statutory language did not create a privilege against discovery because the statutory text and legislative history contained "no indication that Congress intended to prohibit disclosure of [the protected information] in judicial proceedings."[296] Meanwhile, the Tenth Circuit considered both sections of the IRCA, acknowledged that "[o]ne reading of the statute would suggest that *any* disclosure of information is prohibited,"[297] and then, like the Ninth and Eleventh Circuits, concluded that the statutory text did not create an evidentiary privilege.[298] These rulings all recognize that Congress often imposes confidentiality without privilege and that courts should not presume that statutory language abrogates judicial process unless the plain text of the statute requires that result.[299]

*3. Implied Statutory Privileges.* — In contrast to the Ninth, Tenth, and Eleventh Circuits' reasoning, which safeguards the legislated subpoena and discovery rules unless a statute expressly abrogates them,[300] the D.C., Third, and Fifth Circuits recognize a limited, additional route for courts to construe facial silence in statutory text as impliedly creating

---

[291] *Zambrano*, 972 F.2d at 1126.

[292] *Id.* at 1125.

[293] *See In re* Nelson, 873 F.2d 1396, 1397 (11th Cir. 1989).

[294] 873 F.2d 1396.

[295] *See id.* at 1397; 8 U.S.C. § 1160(b)(6)(A)(i)–(iii) (barring "use," "publication," or "permit[ting] anyone . . . to examine" covered information); 8 U.S.C. § 1160(b)(6)(B) (enumerating express exceptions without mentioning judicial process).

[296] *In re* Nelson, 873 F.2d at 1397 (citing St. Regis Paper Co. v. United States, 368 U.S. 208, 218 (1961); Freeman v. Seligson, 405 F.2d 1326, 1351 (D.C. Cir. 1968) (Leventhal, J., concurring)).

[297] United States v. Hernandez, 913 F.2d 1506, 1511 (10th Cir. 1990).

[298] *Id.* at 1512. Notably, whereas the denial of privilege in *Zambrano* and *In re Nelson* served the interests of asylum seekers — the class of people whom the IRCA's statutory confidentiality provisions were presumably designed to protect — the denial of privilege in *Hernandez* had the opposite, detrimental effect on an asylum seeker. *See id.* at 1510–11.

[299] *See generally* IMWINKELRIED, *supra* note 160, § 1.3.7 nn.192–97, 208–15 (collecting cases and secondary authorities); 23A GRAHAM & MURPHY, *supra* note 144, § 5437; WIGMORE, *supra* note 215, § 2377; Mila Sohoni, *The Power to Privilege*, 163 U. PA. L. REV. 487, 497–99 (2015).

[300] *See* Zambrano v. INS, 972 F.2d 1122, 1125–26 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993); *Hernandez*, 913 F.2d at 1512; *In re* Nelson, 873 F.2d at 1397.

privilege.[301] The split arises from divergent readings of the murky middle child in the Supreme Court's trilogy of statutory privilege cases, *Baldrige v. Shapiro*. *Baldrige* is deceptively foggy on this issue. In *Baldrige*, the Court considered the amended section 9(a) of the Census Act and concluded this time around that the text sufficed to create a privilege.[302] Recall that the amended text states: "Copies of census reports which have been so retained *shall be immune from legal process*."[303] The case concerned a civil action in which the City of Denver, Colorado, and Essex County, New Jersey, sought discovery of raw census data from the Census Bureau.[304] The Tenth Circuit had denied discovery, reasoning that the "express prohibitions"[305] in the amended statutory text "make abundantly clear that Congress intended . . . a rigid immunity from . . . discovery."[306] The Supreme Court affirmed.[307] The Court concluded that the amended Census Act "*explicitly* provide[s] for the nondisclosure of" the data[308] and that "[t]his strong policy of nondisclosure indicates that Congress intended the confidentiality provisions to constitute a 'privilege' within the meaning of the Federal Rules."[309]

Given the *Baldrige* Court's emphasis on the statute "explicitly" mandating nondisclosure, it is possible to read the Court's recognition of a privilege as relying on the express "immune from legal process" language from section 9(a)'s amended statutory text. This is the reading that the Ninth Circuit has adopted, concluding that "[t]he provision in *Baldrige* contains an express prohibition against the production of Census information in judicial proceedings," and "judicial disclosure may be prohibited where the statute expressly requires such a result."[310]

To be sure, Congress enacted the express privilege language in response to the issue in *St. Regis*, namely, the scope of protection for census information retained by census respondents,[311] whereas *Baldrige* concerned a different issue that *St. Regis* left unanswered, namely, the scope

---

[301] *See* Cazorla v. Koch Foods of Miss., L.L.C., 838 F.3d 540, 552 (5th Cir. 2016); *In re* England, 375 F.3d 1169, 1178–80 (D.C. Cir. 2004); Pearson v. Miller, 211 F.3d 57, 68 (3d Cir. 2000).

[302] Baldrige v. Shapiro, 455 U.S. 345, 361 (1982).

[303] 13 U.S.C. § 9(a) (emphasis added) (amended after *St. Regis* by Act of Oct. 15, 1962, Pub. L. No. 87-813, 76 Stat. 922).

[304] *Baldrige,* 455 U.S. at 348–50.

[305] McNichols v. Klutznick, 644 F.2d 844, 844 (10th Cir. 1981).

[306] *Id.* at 845. In contrast, the Third Circuit had ordered the Census Bureau to release the data. *Baldrige*, 455 U.S. at 350.

[307] *Baldrige*, 455 U.S. at 362.

[308] *Id.* at 355 (emphasis added).

[309] *Id.* at 361.

[310] Zambrano v. INS, 972 F.2d 1122, 1126 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993).

[311] *See Baldrige*, 455 U.S. at 356 n.11.

of protection for census information possessed by the Department of Commerce.[312] And the *Baldrige* opinion block quoted section 9(a) without including the express privilege language from the amended statutory text.[313] It is therefore uncertain what role, if any, that language played in the Court's reasoning.[314] Even so, it is difficult to imagine that Congress's enactment of express privilege language as a direct override of the *St. Regis* decision would have had no influence on the Court. So it remains possible to characterize *Baldrige*, like the Ninth Circuit does, as construing statutory text that expressly indicates congressional intent to create a privilege.

An alternate plausible reading of *Baldrige* is that the opinion recognizes a narrow route for courts to construe federal statutes as impliedly creating privileges, even without statutory language that expressly exempts information from judicial process. This reading depends on presuming that Congress's enactment of express privilege language directly overriding the *St. Regis* decision did not influence the Court's analysis in *Baldrige*. If one entirely ignores the express privilege language, the analysis can proceed as follows.

Recall that *Baldrige* concerned Denver's and Essex County's efforts to obtain raw census data from the Census Bureau.[315] As mentioned above,[316] section 9(a) of the Census Act contains three broad confidentiality provisions that restrict "use," "publication," and "permit[ting] anyone . . . to examine" covered information.[317] Meanwhile, by the

---

[312] *See supra* note 249 (observing that "the [*St. Regis*] opinion scrupulously avoided language, . . . even in passing dicta," that might be read to characterize the *pre-amended* section 9(a) as creating an evidentiary privilege for information possessed by the Department of Commerce).

[313] *See Baldrige*, 455 U.S. at 354–55 (quoting 13 U.S.C. § 9(a)).

[314] *Cf. id.* at 356 n.11 (citing the 1962 amendment to section 9(a) in the context of concerns about census takers' confidentiality).

[315] *See id.* at 351 (noting that the City of Denver sought judicial discovery of "vacancy information contained in the updated master address registers"); *id.* at 349 (noting that Essex County sought the same information). The Court clarified that the "list of vacant addresses is part of the raw census data . . . reported by or on behalf of individuals." *Id.* at 358.

[316] *See supra* pp. 2760–61 (discussing section 9(a) in relation to *St. Regis*).

[317] At the time of *Baldrige*, section 9(a) of the Census Act stated *in full*:

> Information as confidential; exception
>
> (a) Neither the Secretary, nor any other officer or employee of the Department of Commerce or bureau or agency thereof, or local government census liaison, may, except as provided in section 8 of this title —
>
> (1) use the information furnished under the provisions of this title for any purpose other than the statistical purposes for which it is supplied; or
>
> (2) make any publication whereby the data furnished by any particular establishment or individual under this title can be identified; or
>
> (3) permit anyone other than the sworn officers and employees of the Department or bureau or agency thereof to examine the individual reports.
>
> No department, bureau, agency, officer, or employee of the Government, except the Secretary in carrying out the purposes of this title, shall require, for any reason, copies of census reports which have been retained by any such establishment or individual. Copies of census reports which have been so retained shall be immune from legal process, and

time of the Court's ruling in *Baldrige*, Congress had also amended section 8 and eliminated all of the exceptions permitting disclosure of raw census data to anyone other than the "respondent" who initially provided it.[318] To emphasize, at the time of the Court's ruling, section 8(b) contained *no exceptions* for disclosure of raw census data to anyone else.[319] Considering both amended sections 9(a) and 8(b),[320] the Court recognized that the text imposed "a bar on disclosure of all raw data reported by or on behalf of individuals."[321] It reasoned that this nondisclosure mandate with no exceptions other than returning information to its source "embod[ied] explicit congressional intent to preclude *all*

---

shall not, without the consent of the individual or establishment concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

13 U.S.C. § 9(a) (1976). The current text of section 9(a) is substantially similar. *See* 13 U.S.C. § 9(a).

Note that, if the term "reports" in section 9(a)(3) is construed to mean something different from raw data reported by a census respondent, then the sole confidentiality provisions that apply to raw data are the restrictions on "use" and "publication." Following *Baldrige*, the D.C. Circuit explained that statutory restrictions on "publishing" do *not* suffice to create evidentiary privileges, *In re* England, 375 F.3d 1169, 1180 (D.C. Cir. 2004) (citing Freeman v. Seligson, 405 F.2d 1326, 1349 (D.C. Cir. 1968) (Leventhal, J., concurring)), and federal district courts in Indiana and Massachusetts adopted conflicting interpretations of whether statutory restrictions on "use" of information may do so, *compare* Sajda v. Brewton, 265 F.R.D. 334, 340–41 (N.D. Ind. 2009) (finding that a statute stating that covered information may not be "used in a civil action," *id.* at 140 (quoting 49 U.S.C. § 504(f)), created a discovery privilege), *with* Macaulay v. Mass. Bay Commuter R.R. Co., No. 07cv10864, 2008 WL 11388601, at *2 (D. Mass. June 26, 2008) (holding that a statute stating that covered information "may [not] be used in a civil action" did not create a discovery privilege (quoting 49 U.S.C. § 20903)). Therefore, the most likely source for a section 9(a) privilege in *Baldrige* was the 9(a)(3) restriction on "permit[ting] . . . anyone to examine" census "reports," meaning the same information subject to the express privilege language in the post–*St. Regis* amendment.

318 13 U.S.C. § 8(a). The 1976 Amendment to the Census Act replaced section 8 with its current form. *See* Act of Oct. 17, 1976, Pub. L. No. 94-521, sec. 6, § 8, 90 Stat. 2459, 2460 (codified at 13 U.S.C. § 8). Section 8 now enumerates a series of express exceptions permitting the Secretary of Commerce to disclose aggregated, anonymized statistical reports *derived from* the raw census data, but contains *zero* exceptions that permit disclosure of the raw data itself (other than to the respondent who provided it). *See* 13 U.S.C. § (8)(a)–(b).

319 At the time of *Baldrige* (and currently), section 8(b) stated in relevant part:

> [T]he 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*, and may make special statistical compilations and surveys, for departments, agencies, and . . . other public and private persons . . . .

13 U.S.C. § 8(b) (emphasis added).

320 *See Baldrige*, 455 U.S. at 354–55.

321 *Id.* at 361. The particular raw data at issue in the case were lists of individual addresses reported to the Census Bureau. *Id.* at 347. For contemporary issues concerning disclosure avoidance and census data, see Dan Bouk & danah boyd, Are the Census Data Fit for Purpose? The Entanglement of Politics and Math 20–28 (May 4, 2020) (unpublished manuscript) (on file with the Harvard Law School Library).

disclosure" of that information.[322] It held that "[t]his strong policy of nondisclosure indicate[d] that Congress intended the confidentiality provisions to constitute a 'privilege' within the meaning of the Federal Rules."[323] Thus, *Baldrige* arguably established that, when a statute contains a broad nondisclosure mandate with no express exceptions other than to return information to the source from whence it came, courts may construe that statute as impliedly creating a privilege to block judicial process.

The D.C. Circuit has adopted such an implied privilege reading of *Baldrige*.[324] In *In re England*,[325] authored by then-Judge Roberts, the D.C. Circuit concluded that "[t]he Supreme Court has addressed the question of whether broad, statutory bans on disclosure [not including an express privilege] should be applied according to their terms, when doing so interferes with a civil litigant's effort to obtain discovery of relevant material."[326] Relying on this reading of *Baldrige*, Judge Roberts read an implied privilege into another statute.[327] At that time,[328] the statute stated that board deliberations concerning military personnel promotions "may not be disclosed to any person not a member of the board."[329] The statute then listed a narrow set of exceptions to permit the board to disclose its reports up the chain of command to the President, exceptions which are necessary to effectuate the purpose of the statute as a whole.[330] Judge Roberts reasoned that:

> [T]he drafters of Section 618(f) wrote the ban on disclosure in such broad and absolute terms that they felt the need to specify that board proceedings *could* be disclosed in connection with the very reason you have

---

[322] *Baldrige*, 455 U.S. at 361; *see id.* at 361 n.17.

[323] *Id.* at 361.

[324] Note that, prior to *Baldrige*, the D.C. Circuit had held in *Association for Women in Science v. Califano*, 566 F.2d 339 (D.C. Cir. 1977), that federal statutes "which bar disclosure without specifying from whom they are to be withheld . . . create a qualified privilege." *Id.* *Baldrige* arguably overturned this holding, and *In re England*, 375 F.3d 1169 (D.C. Cir. 2004), did not cite it.

[325] 375 F.3d 1169.

[326] *Id.* at 1178.

[327] *Id.* at 1181 (finding an implied privilege in 10 U.S.C. § 618(f) (2000) (repealed 2006)).

[328] Two years after the *In re England* decision, Congress amended the statute to strike section 618(f) and added an express privilege stating that military selection board proceedings "are immune from legal process; . . . [and] may not be admitted as evidence." John Warner National Defense Authorization Act for Fiscal Year 2007, Pub. L. No. 109-364, sec. 547(a), § 613a(b), 120 Stat. 2083, 2215 (2006) (codified at 10 U.S.C. § 613a(b)); *see id.* at 2216. In searching 120 legislative history documents for section 618(f), I found no reference to the *In re England* opinion.

[329] 10 U.S.C. § 618(f) ("Except as authorized or required by this section, proceedings of a selection board . . . may not be disclosed to any person not a member of the board."); *see In re* England, 375 F.3d at 1170.

[330] *See* 10 U.S.C. § 618(a)–(c), (e) (2000).

> them — to submit recommendations to the Secretary of a military department, the Secretary of Defense, and ultimately the President for action.[331]

He then found this language analogous to sections 8 and 9(a) of the Census Act and read it similarly to "block civil discovery."[332] In *In re England*, then, the D.C. Circuit considered the section 618(f) exceptions to be so narrow that it treated the disclosure prohibition as effectively a categorical bar like the amended Census Act.[333] Hence, the section 618(f) bar could satisfy a narrow route to implied privilege where a statute blanket prohibits disclosure without exception other than returning information to its source. The Third and Fifth Circuits have adopted similar reasoning, though without as thorough of an analysis.[334]

The upshot of the current doctrine, then, is that the *St. Regis* "duty to avoid a construction that would suppress otherwise competent evidence"[335] controls. The Ninth, Tenth, and Eleventh Circuits require that statutes contain express privilege language before courts may construe them as blocking judicial process.[336] The D.C., Third, and

---

331 *In re* England, 375 F.3d at 1177.

332 *Id.* at 1181 ("As in *Baldrige*, we accordingly apply the bar on disclosure as written, and conclude that it applies to block civil discovery . . . ."); *see id.* at 1178–80.

333 A less generous reading is that section 618(f) falls beyond the scope of *Baldrige* because it includes an exception permitting disclosure to someone other than the source. *See id.* at 1177. Note that section 618(f) is also distinguishable from section 9(a) of the Census Act because section 618(f) controls information at its original source, whereas section 9(a) controls information one hop away — in the possession of the Census Bureau.

334 *See* Pearson v. Miller, 211 F.3d 57, 68 (3d Cir. 2000) ("Statutory provisions providing for duties of confidentiality do not automatically imply the creation of evidentiary privileges binding on courts. . . . It does not follow, however, that a statute providing for a duty of confidentiality — but lacking an express provision for an evidentiary privilege, per se — could not also be interpreted as creating such a privilege."); Cazorla v. Koch Foods of Miss., L.L.C., 838 F.3d 540, 550–52, 551 n.29 (5th Cir. 2016). *Cazorla v. Koch Foods of Mississippi*, 838 F.3d 540, is difficult to square with *St. Regis*, *Baldrige*, and *In re England* alike. In *Cazorla*, the Fifth Circuit, citing *In re England*, read an implied privilege into a statute that protects confidentiality of certain immigration information. *Id.* at 550, 552. The statute at issue in the case, 8 U.S.C. § 1367, states in relevant part: "Except as provided in subsection (b) of this section, in no case may the Attorney General . . . permit use by or disclosure to anyone . . . of any information which [is covered by the statute]." *Id.* at 550 (quoting 8 U.S.C. § 1367(a)). Unlike the statutes at issue in *Baldrige* and *In re England*, this statute contains eight enumerated exceptions that permit disclosure in a wide array of circumstances. *See* 8 U.S.C. § 1367(b)(1)–(8) (listing exceptions, including for "judicial review of a determination [of admissibility or deportability of an alien]," but not including court orders, discovery orders, or subpoenas pertaining to other cases or controversies). It is thus difficult to see how this statute could "embody explicit congressional intent to preclude *all* disclosure," Baldrige v. Shapiro, 455 U.S. 345, 361 (1982), or to otherwise harmonize the *Cazorla* holding with the *St. Regis* strict construction mandate, *see* St. Regis Paper Co. v. United States, 368 U.S. 208, 218 (1961).

335 *St. Regis*, 368 U.S. at 218.

336 Zambrano v. INS, 972 F.2d 1122, 1125 (9th Cir. 1992), *vacated and remanded on other grounds*, 509 U.S. 918 (1993); United States v. Hernandez, 913 F.2d 1506, 1511 (10th Cir. 1990); *In re* Nelson, 873 F.2d 1396, 1397 (11th Cir. 1989).

Fifth Circuits take the contrary position and recognize a narrow additional route to implied statutory privileges.[337] Even in these latter jurisdictions, however, facial silence in statutory text should remain insufficient to construe a statute as creating a privilege unless the statute contains no, or virtually no, express exceptions for permissible disclosures and thus embodies "explicit congressional intent to preclude *all* disclosure of" that information.[338]

*4. Misconstruing the Stored Communications Act.* — Twenty-first-century courts construing SCA section 2702 to block criminal defense subpoenas have gotten it wrong. The current case law is inconsistent with Supreme Court doctrine and both sides of the federal circuit split over express and implied statutory privileges.

As a threshold matter, "[t]he party claiming privilege has the burden to establish its existence."[339] Technology companies seeking to quash criminal defense subpoenas under section 2702 have failed to meet that burden. Indeed, it appears that few, if any, have even tried, meaning that courts should have automatically ruled that no privilege applied. Facebook's recent petition for certiorari before the Supreme Court in *Facebook, Inc. v. Superior Court*[340] illustrates this repeat oversight of the burden of claiming privilege. Facebook's petition never once mentions the word "privilege" and fails to cite any of the three leading Supreme Court cases on the issue of when courts must, and must not, read federal statutes as creating a privilege: *Pierce*, *Baldrige*, and *St. Regis*.[341] Also illustrative is a recent case from the District of Columbia Court of Appeals, *Facebook, Inc. v. Wint*.[342] In *Wint*, Facebook argued that section 2702 barred it from complying with a criminal defendant's subpoenas to Facebook and Instagram.[343] Facebook's opening brief before the District of Columbia Court of Appeals never asserted that the SCA creates an evidentiary privilege.[344] Nor did it cite *Pierce*, *Baldrige*, or *St. Regis*.[345] Instead, Facebook presented a classic *expressio unius*

---

[337] *See Cazorla*, 838 F.3d at 552; *In re* England, 375 F.3d at 1180; *Pearson*, 211 F.3d at 68.

[338] *Baldrige*, 455 U.S. at 361.

[339] Friedman v. Bache Halsey Stuart Shields, Inc., 738 F.2d 1336, 1341 (D.C. Cir. 1984) (citing Black v. Sheraton Corp. of Am., 564 F.2d 531, 547 (D.C. Cir. 1977)).

[340] 140 S. Ct. 2761 (2020).

[341] *See generally* Petition for a Writ of Certiorari, *supra* note 7.

[342] 199 A.3d 625 (D.C. 2019).

[343] *Id.* at 628; Facebook, Inc.'s Motion for Summary Reversal at 2–3, *Wint*, 199 A.3d 625 (No. 18-ss-958).

[344] *See generally* Facebook, Inc.'s Motion for Summary Reversal, *supra* note 343. Although Facebook cited a prior District of Columbia Court of Appeals case relating to "evidentiary privileges," *id.* at 18 (quoting Anderson v. United States, 607 A.2d 490, 495 (D.C. 1992)), it proceeded to characterize the SCA as containing "prohibitions on disclosure," *id.*

[345] *See generally id.*

argument for how to interpret the statutory text.[346] It spent the rest of its brief arguing that this interpretation of the statute was not unconstitutional as applied,[347] and that the defendant had failed to meet *his* presumed burden of showing a constitutional need to overcome the SCA statutory bar.[348]

Given this repeat absence of briefing on privilege law,[349] it should not be surprising that federal appellate and state supreme court opinions on the SCA subpoena bar have entirely overlooked the doctrine governing statutory privilege construction. For instance, in *Facebook, Inc. v. Superior Court* (*Hunter*),[350] the California Supreme Court contemplated the SCA bar on criminal defense subpoenas without mentioning evidentiary privileges, *Pierce*, *Baldrige*, or *St. Regis*.[351] Nor have key civil cases that construed section 2702 to bar civil subpoenas addressed the mandatory statutory interpretation rules for privileges. *O'Grady*, decided three years after *Pierce*, did not mention that case.[352] Worse, it incorrectly stated that there was no authority directly on point for how courts must construe section 2702(a) in relation to subpoena power.[353] *O'Grady* did not even discuss the general principle that evidentiary privileges must be construed narrowly, much less the specific manifestation of that principle in a strict construction rule for federal statutory privileges.[354]

Even absent waiver, construing the SCA as creating a privilege that blocks criminal defense subpoenas is inconsistent with the rules that govern statutory privilege construction. Starting with the statute's plain text, SCA section 2702(a) contains a broad nondisclosure mandate stating: "[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the

---

346 *See id.* at 10.

347 *Id.* at 11–20.

348 *Id.* at 19–20, 19 n.13.

349 Criminal defense counsel challenging the SCA have referenced privilege, but have generally argued that defendants' constitutional rights should *defeat* any claim to privilege, without pointing out that courts must read the SCA according to the special statutory construction rules for privileges. *See, e.g.*, Real Parties Lee Sullivan and Derrick Hunter's Opening Brief on the Merits at 18, Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725 (Cal. 2018) (No. S230051). The defense briefs in *Wint* are an exception and raised a statutory argument similar to that developed in this Article. *See* Brief for the United States, *supra* note 2, at 16–28. As noted, the District of Columbia Court of Appeals did not resolve this issue. *See supra* pp. 2737–38.

350 417 P.3d 725.

351 *See generally id.*

352 *See generally* O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72 (Ct. App. 2006).

353 *See id.* at 85–86.

354 *See id.* at 85–89.

contents of a communication while in electronic storage by that service."[355] The statute nowhere states that communications contents possessed by technology companies "shall be immune from legal process,"[356] shall be "privileged as an evidentiary matter,"[357] "shall not be subject to discovery,"[358] or any of the other common formulations that Congress regularly uses to enact statutory evidentiary privileges.[359] Section 2702(a) never mentions privilege, discovery, criminal subpoenas, court orders, admissibility, or any remotely similar language. Nor does the statute generally preclude all disclosures of covered information. On the contrary, section 2702(b) lists nine express exceptions for permissible disclosures, including disclosures to an intended recipient of the communication, disclosures necessary to the rendition of the service, and disclosures to governmental entities.[360] Hence, section 2702 falls squarely into the ambiguous category of statutes with confidentiality provisions that are silent as to their effect on otherwise-valid judicial compulsory process.[361]

In a misguided, if well-meaning, effort at judicial restraint, courts faced with the task of construing section 2702's ambiguous silence as to privilege have mistakenly applied *expressio unius* principles of statutory construction. In general, *expressio unius* counsels courts against reading silence in a statute that lists some express exceptions to imply additional exceptions not listed.[362] Accordingly, courts have held that because section 2702 expressly enumerates certain permissible disclosures but is silent on criminal defense subpoenas, the statute does not permit disclosures pursuant to such subpoenas.[363] But *expressio unius* is the wrong principle to apply. Instead, courts should apply the *St. Regis* strict construction rule that courts have a "duty to avoid a construction that would suppress otherwise competent evidence unless the statute, strictly construed, *requires such a result*."[364] The plain text of section 2702 does not "require" a result that would "suppress otherwise competent evidence" by blocking criminal defense subpoenas because there is a reasonable, alternate, nonprivilege reading of the SCA's statutory text. Courts could — and therefore should — read section 2702 to mandate *confidentiality* in nonlitigation contexts, yet yield to judicial compulsory process.

---

355 18 U.S.C. § 2702(a)(1).
356 22 U.S.C. § 3144(d).
357 15 U.S.C. § 7215(b)(5)(A).
358 23 U.S.C. § 148(h)(4).
359 *See supra* notes 256–268 and accompanying text.
360 18 U.S.C. § 2702(b)(1)–(9).
361 *See supra* notes 244–251 and accompanying text.
362 *See* Gluck & Bressman, *supra* note 221, at 924.
363 *See, e.g.*, Facebook, Inc. v. Wint, 199 A.3d 625, 628, 633–34 (D.C. 2019).
364 St. Regis Paper Co. v. United States, 368 U.S. 208, 218 (1961) (emphasis added).

Considering the issue from either side of the current federal circuit split on implied statutory privileges leads to the same conclusion. The Ninth, Tenth, and Eleventh Circuits have taken the position that a statute must expressly indicate congressional intent to create a privilege before a court may construe it to block judicial process.[365] Section 2702 does not contain any express privilege language, so the express privilege rule would flatly preclude courts from construing the SCA to bar criminal defense subpoenas.

Meanwhile, reading section 2702 as creating a privilege is also inconsistent with the narrow route to implied statutory privileges that the D.C., Third, and Fifth Circuits have recognized.[366] As explained above, that route relies on reading *Baldrige* as an implied privilege case. But the statute at issue in *Baldrige* barred all disclosures of covered information without exception apart from returning information to its source.[367] And the Court relied on that fact to hold that the statute "embod[ied] explicit congressional intent to preclude *all* disclosure of" the information.[368] Similarly, the statute at issue in the D.C. Circuit's *In re England* case barred all disclosures without exception apart from relaying military promotion decisions up the chain of command to the President,[369] an exception that the D.C. Circuit concluded was necessary to effectuate the very purpose of the statute (to make military promotions).[370] In contrast, the SCA has a plethora of exceptions permitting disclosures in a wide variety of circumstances, including to subscribers, to employees, to protect property rights, and for business purposes "incident to the rendition of the service."[371] Thus, the SCA does not comfortably fit the D.C. Circuit's implied privilege route.

Finally, on either side of the circuit split, there is a strong presumption against reading a statute to create a privilege. Commentators have concluded that "[s]trong legislative history would probably be necessary

---

[365] *See supra* notes 282–299 and accompanying text (explaining the rule in express privilege jurisdictions).

[366] As explained above, the Third and Fifth Circuits have recognized implied statutory privileges but without as thorough of an analysis as the D.C. Circuit. *See supra* note 334. The Fifth Circuit's holding in *Cazorla* is particularly challenging to square with *St. Regis*, and thus courts should not rely on it for guidance in construing SCA section 2702. *See supra* note 334.

[367] *See* 13 U.S.C. § 9(a).

[368] Baldrige v. Shapiro, 455 U.S. 345, 361 (1982).

[369] 10 U.S.C. § 618(a)–(c) (2000); *see In re* England, 375 F.3d 1169, 1177 (D.C. Cir. 2004) (noting that, at that time, the pertinent nondisclosure provision of the statute stated, in full: "Except as authorized or required by this section, proceedings of a selection board convened under section 611(a) of this title may not be disclosed to any person not a member of the board" (quoting 10 U.S.C. § 618(f) (repealed 2006))).

[370] *See* 375 F.3d at 1177.

[371] 18 U.S.C. § 2702(b)(5); *see id.* § 2702(b)(1)–(9).

to overturn the presumption" against reading statutes to create privileges.[372] Section 2702 of the SCA lacks such legislative history. The congressional records documenting the 1986 consideration and passage of the bill in both the House and Senate, as well as the House and Senate Judiciary Committee reports, all discussed governmental entities' access to communications contents through warrants, court orders, and administrative and grand jury subpoenas, but all are silent on criminal defense subpoenas.[373] Similarly, multiple congressional hearings in the years leading up to the passage of the SCA discussed law enforcement subpoenas, including administrative and grand jury subpoenas, with virtually no mention of criminal defense subpoenas.[374] There are two possible exceptions to the general absence of any consideration of defense investigations. In a 1985 hearing, two witnesses sought clarification as to whether the content disclosure bar would apply to nongovernmental subpoenas.[375] And in a 1984 hearing, one witness referenced magazine articles describing a legal case in which the owner of a theater subpoenaed lists of people who had viewed adult movies on TV in order to defend himself against obscenity charges for screening the same movies in his theater.[376] Those three passing comments, amid thousands of pages of testimony, did not make it into either the House or Senate Judiciary Committee Reports or the congressional record.

---

372 IMWINKELRIED, *supra* note 160, § 1.3.7 (footnote omitted).

373 *See* S. REP. NO. 99-541, at 38 (1986); H.R. REP. NO. 99-647, at 68 (1986); 132 CONG. REC. 27,635 (1986); 132 CONG. REC. 28,126 (1986) (not mentioning nongovernmental entities' access to contents, whether criminal defendants or civil litigants).

374 *See, e.g.*, *Electronic Communication Privacy: Hearing on S. 1667 Before the Subcomm. on Pats., Copyrights & Trademarks of the S. Comm. on the Judiciary*, 99th Cong. 154 (1985) [hereinafter *Hearing on S. 1667*] (discussing civil and grand jury subpoenas with no mention of criminal defense subpoenas); *Surveillance: Hearings on the Matter of Wiretapping, Electronic Eavesdropping, and Other Surveillance Before the Subcomm. on Cts., C.L. & the Admin. of Just. of the H. Comm. on the Judiciary*, 94th Cong. 476–77, 502 (1975) (discussing law enforcement and grand jury subpoenas with no mention of criminal defense subpoenas).

375 *See Hearing on S. 1667*, *supra* note 374, at 99 (statement of Philip M. Walker, Vice Chairman, Electronic Mail Association) ("[W]e are unclear at this time whether [the] bill . . . would apply to the subpoena of electronic messages in certain civil lawsuits."); *id.* at 102, 105 (statement of P. Michael Nugent, Chairman, Committee on Computer Systems & Communications Privacy, ADAPSO) (commenting that "the law is, at best, unclear," *id.* at 102, and mentioning ambiguity concerning disclosure of contents "to both governmental and non-governmental parties in both criminal and civil litigation," *id.* at 105).

376 *See 1984: Civil Liberties and the National Security State: Hearings Before the Subcomm. on Cts., C.L. & the Admin. of Just. of the H. Comm. on the Judiciary*, 98th Cong. 278–79 (1984) (statement of Robert Ellis Smith, Publisher, Privacy Journal) [hereinafter *Hearing on 1984*]; *The High-Tech Threat to Your Privacy*, CHANGING TIMES, Apr. 1983, at 61, 62–63, *reprinted in Hearing on 1984*, *supra*, at 285; Richard M. Neustadt & M. Anne Swanson, *Privacy and Videotex Systems*, BYTE, July 1983, at 96, 96, *reprinted in Hearing on 1984*, *supra*, at 290.

Taken together, the legislative history contains ample evidence to show that Congress intended to regulate law enforcement investigations when it enacted the SCA, but not that Congress also intended to obstruct criminal defense investigations.[377]

In sum, construing the SCA to block criminal defense subpoenas violates the rules that govern statutory privilege construction.

## III. THE POLICY OF AN INTERNET COMMUNICATIONS PRIVILEGE

This Part examines policy arguments for and against the current, erroneous SCA privilege and concludes that the privilege is unjustified. As section A explains, those defending the current case law often deploy privacy rhetoric. Yet, on close examination, the existing SCA privilege offers scant privacy protections. Instead, it gifts a court-created subsidy to technology companies and their data-mining markets.

Of course, Congress could amend the SCA to create a novel evidentiary privilege that blocks criminal defense subpoenas to technology companies.[378] And federal courts could use their common law authority to do the same,[379] so long as they first perform the careful balancing of competing interests required to recognize a new common law privilege.[380] Accordingly, section B examines the policy pros and cons of creating a privilege for the internet. It argues that shielding internet communications from criminal defense subpoenas without regard to the subject matter of the communications or the communicants' expectations of confidentiality would create a vastly overbroad, outlier privilege. Further, it would fail the leading theoretical and doctrinal criteria for justified privileges. While concededly within the power of either Congress or the courts, privileging an entire *medium* of communication would be both unprecedented and unwise.

---

[377] Zwillinger and Genetski's review of the legislative record led them to conclude that "nothing in the legislative history suggests that Congress contemplated, much less intended [to block criminal defense subpoenas]. . . . Congress appears simply to have overlooked the potential concerns of non-state actors seeking compulsory access to information held by ISPs." Zwillinger & Genetski, *supra* note 10, at 577.

[378] The same is true for civil and administrative subpoenas, or any other valid legal process that is less than constitutionally guaranteed.

[379] *See* FED. R. EVID. 501.

[380] *See* sources cited *supra* notes 225–449.

### *A. Correcting the Current Case Law*

*1. Privacy Interests.* — Facebook recently told the Supreme Court that permitting criminal defendants to subpoena technology companies for electronic communications contents would "threaten[] the privacy interests of millions of Americans."[381] This position does not withstand careful scrutiny. Correcting the case law to eliminate the current SCA privilege would instead make more *nonprivate*, relevant evidence available in criminal cases, with minimal costs to privacy.

To see why, consider three groups of people: those without legitimate privacy interests in subpoenaed information, those with legitimate privacy interests in that information, and those whose privacy interests in the information are unknown. If the erroneous SCA privilege were eliminated, the first group — those without legitimate privacy interests — would lose control over relevant evidence that they could otherwise withhold from the courts. Yet that loss of control would impose zero cost to privacy. This is because current readings of the SCA enable people to withhold evidence from criminal proceedings for reasons entirely unrelated to privacy. For instance, account holders can withhold evidence by residing abroad such that they are beyond the subpoena jurisdiction of U.S. courts,[382] by being dangerous such that subpoenaing them would risk a threat to someone's life or physical safety, by being unreliable such that subpoenaing them would risk their tampering with or destroying evidence, or simply by refusing to obey a subpoena and being held in contempt.[383] In those circumstances, properly enforcing subpoenas to technology companies would make more relevant evidence available without affecting privacy.

Meanwhile, the second group — those with legitimate privacy interests — would largely retain their status quo privacy protections. Recall that current readings of the SCA already permit criminal defendants (and nongovernmental civil litigants) to subpoena individuals directly for their communications contents.[384] Individuals who wish to challenge such a subpoena must affirmatively move to quash it in court.[385] Judges may either quash subpoenas that are unduly privacy invasive[386] or impose protective orders that restrict the use and dissemination of information disclosed to defense counsel.[387] If the subpoenas were served on technology companies instead, individuals would retain

---

381 Petition for a Writ of Certiorari, *supra* note 7, at 15 (capitalization omitted).

382 *See* sources cited *supra* note 3.

383 *See supra* p. 2741.

384 *See supra* p. 2740.

385 *See* FED. R. CRIM. P. 17(c)(2).

386 *See* Wexler, *supra* note 52 (manuscript at 13).

387 *Cf.* Pearson v. Miller, 211 F.3d 57, 72 (3d Cir. 2000) ("Legitimate interests in privacy are among the proper subjects of [a protective order].").

identical standing to move to quash and seek these same privacy protections.[388]

Of course, before anyone can move to quash a subpoena, they first need notice of the subpoena. But the current SCA case law does not guarantee such notice. Currently, defense counsel investigating an individual may subpoena that person's communications from any other account holder with whom the person communicated.[389] In that circumstance, no one is obliged to notify the person being investigated.[390] The other account holder can comply with the subpoena entirely behind the back of the person who is under investigation.[391]

In contrast, many technology companies do have voluntary, contractual, and perhaps even fiduciary,[392] obligations to notify account holders whose records are subject to the service of legal process.[393] Moreover,

---

[388] 81 BARBARA J. VAN ARSDALE ET AL., AMERICAN JURISPRUDENCE § 11 (2d ed.) (Westlaw) (last visited Apr. 10, 2021) ("[Any] person has standing to challenge a subpoena directed to a third party, as long as that person asserts a personal right, privilege, or proprietary interest in the materials being sought by the subpoena."); *see also* Trump v. Vance, 941 F.3d 631, 642 n.15 (2d Cir. 2019) ("When the objection to a subpoena pertains to the information sought, there is little difference between the custodian and the true party in interest, and either may resist enforcement."), *aff'd*, 140 S. Ct. 2412 (2020); Benjamin E. Rosenberg & Robert W. Topp, *The By-Ways and Contours of Federal Rule of Criminal Procedure 17(c): A Guide Through Uncharted Territory*, 45 CRIM. L. BULL. 3, 26–30 (2009) (discussing the government's standing to move to quash defense subpoenas).

[389] Notably, this also means that the current SCA case law does not stop rogue defense counsel from harassing and intimidating witnesses, victims, or others by serving frivolous or abusive subpoenas on them, along with their family, friends, and acquaintances.

[390] Under current law, when a subpoena is served on one individual, no one is obligated to notify the other people whose communications are thereby disclosed. *See* FED. R. CRIM. P. 17. There is an exception requiring *courts* to provide for notice to victims when *either* prosecutors or defendants subpoena sensitive information about the victim from a third party, regardless of whether that third party is a technology company, or any other person or entity. *See id.* 17(c)(3).

[391] By way of illustration, a defendant in California recently attempted to subpoena Facebook, Instagram, and Twitter for messages from a prosecution witness's social media accounts, after a judge determined that the witness herself was not a viable source for the records. Facebook, Inc. v. Superior Ct. (*Hunter*), 259 Cal. Rptr. 3d 331, 334–36 (Ct. App. 2020). Due to the current SCA subpoena bar, the appellate court instructed the defendant to instead subpoena those same messages from other individuals with whom the prosecution witness had communicated. *See id.* at 339 (recommending that defense counsel serve subpoenas on other account holders with whom the subject of their investigation communicated).

[392] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1205–09 (2016); Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346 [https://perma.cc/F226-LBGY]. The question whether technology companies owe duties as information fiduciaries continues to be a topic of recent debate. *See* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 501 (2019); Andrew F. Tuch, *A General Defense of Information Fiduciaries*, 98 WASH. U. L. REV (forthcoming 2021).

[393] *See, e.g.*, *Information for Law Enforcement Authorities*, FACEBOOK, https://www.facebook.com/safety/groups/law/guidelines [https://perma.cc/PDQ6-Q8E9]; *Cloudflare Transparency Report*, CLOUDFLARE, https://www.cloudflare.com/transparency [https://perma.cc/JM9G-EUQH]; *Legal Request FAQs*, TWITTER, https://help.twitter.com/en/rules-and-policies/twitter-legal-faqs [https://perma.cc/AD4F-HUGS].

technology companies' obligations to provide such notice could be further formalized via laws or regulations, an approach with longstanding precedents.[394] Hence, properly enforcing criminal defense subpoenas to technology companies could increase the likelihood that individuals with legitimate privacy interests will receive notice of subpoenas that seek their communications contents.

Putting technology companies in the loop could also encourage the companies to help account holders access the courts, such as by providing information, other resources, and expertise that individuals who are targets of criminal defense subpoenas may otherwise lack. Put another way, channeling subpoenas to technology companies could encourage the legal "haves" to help defend the privacy interests of the legal "have-nots."[395]

Concededly, persons in the third and final group — those whose privacy interests are unknown because, for instance, they cannot be located or contacted — would lose control over information with unknown privacy value. But courts should not protect unknown privacy interests with an unqualified bar on criminal defense subpoenas. Doing so blocks access to private and nonprivate evidence alike. And the hypothetical privacy interests of this third and final group are, by definition, unjustified by any legal showing.[396] Speculative privacy interests that no one has raised in court should not outweigh the sober need for relevant evidence in criminal proceedings.

---

[394] Multiple privacy laws require entities to notify affected individuals about the service of legal process. Some oblige service providers to give notice, *see, e.g.*, HIPAA Disclosure Rules, 45 C.F.R. § 164.512(e) (2019), others the party serving the subpoena, *see* Right to Financial Privacy Act of 1978 (RFPA), 12 U.S.C. § 3405, and still others the court, *see* FED. R. CRIM. P. 17(c)(3). There are also state regulations that impose similar obligations. For instance, while California statutory law does not require public utility service providers to notify customers of service of legal process, *see* DEIRDRE K. MULLIGAN, LONGHAO WANG & AARON J. BURSTEIN, CAL. INST. FOR ENERGY & ENV'T, PRIVACY IN THE SMART GRID: AN INFORMATION FLOW ANALYSIS 25 & n.91 (2011), the California Public Utilities Commission regulatory agency does, *see* Decision Adopting Rules to Protect the Privacy and Security of the Electricity Usage Data of the Customers of Pacific Gas and Electric Company, Southern California Edison Company, and San Diego Gas & Electric Company, No. 11-07-056, at 151, 153, 154–55 (Cal. Pub. Utils. Comm'n July 28, 2011), https://docs.cpuc.ca.gov/word_pdf/FINAL_DECISION/140369.pdf [https://perma.cc/YDZ7-Y2WG].

[395] Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95, 104 (1974). *But cf.* Facebook, Inc. v. Wint, 199 A.3d 625, 631 (D.C. 2019) (concluding that, by channeling defense subpoenas away from internet companies, the SCA privilege "increases the chances that affected individuals can assert claims of privilege or other rights of privacy before covered communications are disclosed to criminal defendants in response to subpoenas"). *See generally* Galanter, *supra* (considering the structural limits of our legal system for making litigation redistributive).

[396] The party asserting a privilege to withhold relevant evidence from the courts bears the burden of proving its existence. *See supra* p. 2773.

Quite importantly, criminal defense subpoena procedures already have substantial, baseline privacy safeguards built in that routinely protect sensitive information implicated in criminal cases — from personal diaries to financial records to location histories to intimate communications between friends and family.[397] Criminal defense subpoenas are subject to judicial review and — unlike warrants — to predisclosure adversarial challenge.[398] While the precise procedures differ by jurisdiction, defense counsel generally must satisfy challenging threshold burdens to enforce a subpoena.[399] And, as mentioned, judges may quash subpoenas that are unduly privacy invasive, or impose strict protective orders that limit the use and dissemination of sensitive information.[400] Correcting the current SCA case law, then, would not eliminate privacy protections. It would merely subject technology companies to standard judicial process and privacy safeguards.

These arguments together show that the current SCA case law is at best a vastly overbroad privacy protection that suppresses relevant, exculpatory evidence from the courts. Enforcing criminal defense subpoenas to technology companies could avoid that harm by making more nonprivate evidence available with minimal costs to legitimate privacy interests.

*2. Service Provider Interests.* — The primary effect of the current SCA privilege is not to protect privacy but, rather, to exempt technology companies from the administrative burdens of complying with subpoenas.[401] The current SCA case law is thus, in effect, a subsidy that courts have gifted to technology companies and their data-mining

---

[397] For a detailed discussion of these safeguards, see Wexler, *supra* note 52 (manuscript at 12–17).

[398] *See id.* (manuscript at 13–14, 40); *see also* FED. R. CRIM. P. 17(c).

[399] For instance, to obtain a pretrial subpoena, most federal courts require criminal defense counsel to first identify the documents they seek with "specificity," and to show that those documents will be both "relevant" and "admissible." United States v. Nixon, 418 U.S. 683, 700 (1974). Similarly, the California Supreme Court recently elaborated a multifactor test to determine whether to enforce a criminal defense subpoena, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 392–94 (Cal. 2020), including among other factors consideration of "a third party's 'confidentiality or privacy rights,'" *id.* at 393 (quoting City of Alhambra v. Superior Ct., 252 Cal. Rptr. 789, 799 (Ct. App. 1988)); *see also id.* at 391 (emphasizing that the records themselves must be returned to the court and not directly to defense counsel).

[400] *See* FED. R. CRIM. P. 17(c)(2), 49.1(e).

[401] Courts have recognized this effect of the SCA privilege but have wrongly attributed it to Congress. The California Supreme Court, for instance, recently commented that "Congress significantly limited the potential onus on providers by establishing a scheme under which a provider is effectively prohibited from complying with a subpoena issued by a nongovernmental entity — *except* in specified circumstances." Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 755 (Cal. 2018).

markets.[402] It is unclear why these companies should receive this special treatment when other companies and private individuals all must shoulder the public duty of supplying relevant evidence to the courts.[403]

To put it more pointedly, rather than protect privacy, the current SCA subsidy protects technology companies' privacy-invasive business practices.[404] As the San Diego District Attorney recently pointed out in arguing that the SCA should *not* block criminal defense subpoenas to Facebook, Facebook's business model includes mining and analyzing the contents of its users' communications.[405] Facebook requires its account holders to grant the company "a non-exclusive, transferable, sublicensable, royalty-free, and worldwide license" to the content they upload,[406] which the company then uses to fuel its advertising business.[407] Further, while Facebook was arguing to block criminal defense subpoenas at every level of the state and federal judiciaries, the company simultaneously engaged in repeat violations of its own users' privacy that resulted in a $5 billion fine by the Federal Trade Commission.[408]

Nor does the large scale of many electronic communication service providers justify the current SCA subsidy. Large companies in other markets successfully manage the burdens of complying with criminal

---

[402] Thank you to Professor Aziz Huq for suggesting that the entitlement courts have afforded to internet companies via the current SCA privilege is, in effect, a subsidy for secondary data markets.

[403] *Cf.* Branzburg v. Hayes, 408 U.S. 665, 688 (1972) (discussing the general public duty to respond to legal process in criminal cases).

[404] *See, e.g.*, 18 U.S.C. § 2702(b) (permitting disclosures to employees and to protect business and proprietary interests of service providers); *see also* Kenneth A. Bamberger et al., *Can You Pay for Privacy? Consumer Expectations and the Behavior of Free and Paid Apps*, 35 BERKELEY TECH. L.J. 327, 330–32 (2020) (discussing digital services companies' business models of data collection and sales); Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1377–78 (2013) (describing the Gmail business model of scanning contents of emails to serve targeted advertisements); *cf.* Michael Birnhack & Niva Elkin-Koren, *Does Law Matter Online? Empirical Evidence on Privacy Law Compliance*, 17 MICH. TELECOMMS. & TECH. L. REV. 337, 364–69 (2011) (documenting Israeli websites' poor compliance with Israeli privacy laws).

[405] *See* San Diego County District Attorney Intervenor Brief at 12–15, Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383 (Cal. 2020) (No. S245203).

[406] *Terms of Service*, FACEBOOK, https://www.facebook.com/terms.php [https://perma.cc/KRU8-JZVD]; *see* San Diego County District Attorney Intervenor Brief, *supra* note 405, at 10.

[407] *See* San Diego County District Attorney Intervenor Brief, *supra* note 405, at 12.

[408] Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/9QM6-DEJP].

defense subpoenas, including telephone companies,[409] banks,[410] and hospitals.[411] Moreover, the burdens of subpoena compliance are tailored to avoid antitrust problems, since startups and smaller companies that possess less data can expect to receive fewer subpoenas than their larger incumbent competitors.[412] Perhaps more concretely, technology companies have flourished[413] despite the fact that current interpretations of the SCA already require them to comply with criminal defense and civil subpoenas for noncontent records,[414] civil subpoenas seeking an opposing party's communications contents,[415] and law enforcement subpoenas and warrants.[416] Compliance with the smaller number of criminal defense subpoenas would add a comparatively minor burden. And, of course, if any individual criminal defense subpoena were to be "unreasonable or oppressive,"[417] technology companies could move to quash on that basis.[418]

Indeed, the scale of many technology companies should give courts yet another reason to *not* construe the SCA as impliedly creating a privilege for those companies to block criminal defense subpoenas.[419] Technology companies are a concentrated interest group with far more

---

409 *See, e.g.*, United States v. Martin, No. 07-CR-51, slip op. at 4, 10 (E.D. Tenn. Dec. 23, 2008) (upholding criminal defense subpoena seeking nonparty's cell-site location information).

410 The Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3423, imposes no limitations on criminal defense subpoenas to financial services intermediaries seeking records for clients other than the defendant. *See id.*

411 HIPAA permits criminal defense subpoenas seeking medical and mental-health records for a patient other than the defendant. *See* 45 C.F.R. § 164.512(e)(1)(vi) (2019).

412 *Cf.* Mark A. Lemley & Mark P. McKenna, *Unfair Disruption*, 100 B.U. L. REV. 71, 83–90 (2020) (discussing incumbents' use of litigation to block new market entrants). By contrast, the burden of litigating or complying with subpoenas would not help incumbents block new market entrants if newer, smaller companies were less likely to share that burden.

413 *See generally* MAKADA HENRY-NICKIE, KWADWO FRIMPONG & HAO SUN, BROOKINGS INST., TRENDS IN THE INFORMATION TECHNOLOGY SECTOR (2019), https://www.brookings.edu/research/trends-in-the-information-technology-sector [https://perma.cc/HMB2-32V8].

414 *See* 18 U.S.C. §§ 2702–2703 (imposing no restrictions on nongovernmental subpoenas seeking noncontent records).

415 On the SCA and civil litigants' subpoena power, see *supra* notes 114–116 and accompanying text.

416 *See* sources cited *supra* note 393.

417 FED. R. CRIM. P. 17(c)(2).

418 *See id.* For instance, in circumstances where defense counsel could subpoena an account holder directly, but chooses to serve the subpoena on a technology company instead, the company would be free to argue that the defendant's alternate available means to obtain the evidence renders compliance with the subpoena unreasonable. *See* Facebook, Inc. v. Superior Ct. (*Touchstone*), 471 P.3d 383, 394 (Cal. 2020) (quoting City of Alhambra v. Superior Ct., 252 Cal. Rptr. 789, 799–800 (Ct. App. 1988)).

419 *See supra* pp. 2776–78 (discussing absence of discussion of criminal defense subpoenas or investigations in the SCA's legislative history).

formidable lobbying power than the relatively dispersed and underfunded criminal defense bar.[420] If courts mistakenly construe the SCA against the preferences of those companies, the companies will have a better chance of persuading Congress to correct the error than would the criminal defense bar were the judicial mistake instead to run in the opposite direction.[421]

Technology companies are free to ask Congress to amend the SCA to create a novel, unqualified privilege that entitles them to block criminal defense subpoenas. In the meantime, courts should not construe ambiguous silence in the SCA's current text to gift an entitlement to technology companies that the statute's legislative history indicates they did not even request at the time of enactment.

### *B. Considering a Novel "Medium" Privilege for the Internet*

The preceding discussion has explained why correcting the existing erroneous construction of the SCA's current text would make more relevant, nonprivate evidence available in criminal cases with minimal costs to privacy, while eliminating an apparently unjustified subsidy that courts have supplied to technology companies and their data-mining markets. Nonetheless, if legislators or courts are displeased with the result, options are available to them. Congress could amend the SCA to enact a novel statutory privilege that unqualifiedly bars criminal defendants from subpoenaing technology companies for the contents of another's online communications.[422] Or courts could rely on their common law authority to craft such a privilege from whole cloth,[423]

---

[420] *See* Ryan Tracy, Chad Day & Anthony DeBarros, *Facebook and Amazon Boosted Lobbying Spending in 2020*, WALL ST. J. (Jan. 24, 2021, 5:24 PM), https://www.wsj.com/articles/facebook-and-amazon-boosted-lobbying-spending-in-2020-11611500400 [https://perma.cc/UU43-4Y9K] (noting that Facebook and Amazon "topped all other U.S. companies in federal lobbying expenditures" in 2020).

[421] *See* Jonathan R. Macey, *Promoting Public-Regarding Legislation Through Statutory Interpretation: An Interest Group Model*, 86 COLUM. L. REV. 223, 255 (1986) ("The interest group pressing for enactment of a special interest statute can always go back to Congress after an unfavorable judicial ruling to have the statute clarified."). Thank you to Aziz Huq for suggesting this argument and pointing out Professor Jonathan Macey's work on this issue.

[422] For instance, following the Supreme Court's opinion in *St. Regis*, Congress added an express privilege to the Census Act. Act of Oct. 15, 1962, Pub. L. No. 87-813, 76 Stat. 922 (codified at 13 U.S.C. § 9(a)). And following the D.C. Circuit's opinion in *In re England*, Congress amended the statute to strike 10 U.S.C. § 618(f) and add an express privilege in 10 U.S.C. § 613a(b). *See* John Warner National Defense Authorization Act for Fiscal Year 2007, Pub. L. No. 109-364, § 547(a), 120 Stat. 2083, 2215–16 (2006) (codified at 10 U.S.C.); *cf.* Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 832–36 (2012) (proposing a privilege for self-tracking data stored with service providers).

[423] FED. R. EVID. 501. Notably, if policymakers are concerned about the scope of criminal defense subpoena powers generally — as opposed to solely subpoenas that seek certain categories of information and solely when served on internet companies — the rulemaking committee for the

provided they first undertake the required balancing of the competing interests.[424] Much of the preceding analysis is relevant to assessing the wisdom of either option. This section presents additional considerations drawn from privilege law and theory.

*1. Privacy and Privilege Law's Shared Theoretical Concerns.* — To date, SCA issues have primarily been examined through the lens of information privacy law. But information privacy law and privilege law share certain core theoretical concerns that can help to inform one another. Specifically, both areas of law share concerns about chilling effects and dignitary harms.[425] In privacy law scholarship, risks of chilling effects from law enforcement surveillance garner substantial attention,[426] although the issue arises in other important contexts as well.[427] Critics debate whether empirical evidence supports the theory that people alter, or chill, their behavior in response to privacy risks.[428] Privilege law scholarship entertains similar debates.[429] "Instrumental" arguments for privileges posit that if certain sensitive communications were vulnerable to judicially compelled disclosure, people would be

---

Federal Rules of Criminal Procedure is free to heighten the safeguards built into the baseline subpoena procedures. *See generally* Wexler, *supra* note 52 (manuscript at 12–17) (describing these safeguards).

424 *See* Jaffee v. Redmond, 518 U.S. 1, 9–10 (1996); Trammel v. United States, 445 U.S. 40, 50–51 (1980); *see also infra* pp. 2788–89 (listing factors).

425 *See generally* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 419 (2008) (discussing chilling effects); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1653 (1999); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487–88 (2006) (discussing dignitary harms); Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CALIF. L. REV. 751, 772–73 (1999) (reviewing PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW (1996) and PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS (1998)).

426 *See, e.g.*, Solove, *supra* note 425, at 487–88, 559 (discussing risks that, with excessive law enforcement surveillance, "[p]eople's behavior might be chilled, making them less likely to attend political rallies or criticize popular views," *id.* at 488).

427 For instance, scholars have also developed a chilling-effects theory in relation to invasions of sexual privacy in online abuse and cyberharassment that disproportionately threaten to silence women and marginalized communities. *See* Danielle Keats Citron & Jonathon W. Penney, *When Law Frees Us to Speak*, 87 FORDHAM L. REV. 2317, 2319–20 (2019). Professor Danielle Keats Citron and Jonathon Penney argue that the "expressive function" of "laws combating invasions of sexual privacy" can help to reduce this silencing effect, *id.* at 2320, and present empirical research findings that "cyberharassment laws would have more salutary than chilling effects for online engagement," *id.* at 2330, thus enriching "[p]ublic discourse and broader democratic deliberation," *id.* at 2333.

428 *See* Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 120–29 (2016); *see also* Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 480 (2015); David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1095–100 (2014).

429 *See generally* Edward J. Imwinkelried, *The Historical Cycle in the Law of Evidentiary Privileges: Will Instrumentalism Come into Conflict with the Modern Humanistic Theories?*, 55 ARK. L. REV. 241 (2002).

chilled from making them in the first place.[430] Hence, privileging those types of communications would cost judicial inquiry little relevant evidence, at least in the aggregate and over time.[431] As with privacy law,[432] critics challenge the premise that privileges stave off equal and opposite chilling effects, questioning whether most people are even aware of privilege law, much less rely on it to guide their intimate communications.[433]

Meanwhile, the possibility of dignitary harms, such as "reputational injury," or "causing emotional angst,"[434] also plays a key role in privacy policy,[435] even leading some to argue that privacy law is overly dependent on moral intuition.[436] Privilege law has inspired analogous scholarly debates. "Humanistic" arguments for privileges presume that privileges do impose some costs to judicial truth-seeking, but contend that the costs are justified by countervailing dignitary interests in shielding certain intimate relationships from intrusion by the courts.[437]

Given these parallel theoretical underpinnings of both information privacy law and privilege law, it should not be surprising that privilege law has developed nuanced balancing tests to accommodate policy concerns over chilling effects and dignitary harms and to weigh those concerns against both individual and societal interests in judicial truth-seeking. Those tests can help decisionmakers to assess any proposed new SCA-like rule that would specially exempt technology companies from complying with criminal defense subpoenas. Accordingly, the following discussion considers the issue from a privilege law perspective.

---

430 *Id*. at 248.

431 *See, e.g.*, Swidler & Berlin v. United States, 524 U.S. 399, 408 (1998) ("[T]he loss of evidence admittedly caused by the privilege is justified in part by the fact that without the privilege, the client may not have made such communications in the first place."); Fisher v. United States, 425 U.S. 391, 403 (1976) ("[A privilege] protects only those disclosures . . . which might not have been made absent the privilege."). Of course, even if one accepts the premise fully, the utilitarian justification does not erase the harm to individual litigants in any given case when a privilege renders crucial existing evidence inaccessible.

432 Penney, *supra* note 428, at 120–29.

433 *See* Imwinkelried, *supra* note 429, at 243.

434 Solove, *supra* note 425, at 487.

435 *See* M. Ryan Calo, Essay, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1144–47 (2011).

436 *See, e.g.*, Bryan H. Choi, *A Prospect Theory of Privacy*, 51 IDAHO L. REV. 623, 627–34 (2015) (arguing instead for enhanced incentives-based justifications for privacy protections).

437 *See generally* IMWINKELRIED, *supra* note 160, § 5.1.

*2. Applying Privilege Analysis to the Internet.* — As an initial matter, creating a novel evidentiary privilege for the entire medium of the internet would depart significantly from the norms and precedents of privilege law. Privileging an entire medium would sweep in communications pertaining to nonsensitive subjects made with no expectation of confidentiality. Perhaps for this reason, the medium of communication does not generally affect privilege, whether by creation or defeat. A communication does not achieve privilege protection by virtue of having been written on a paper and locked inside a drawer, recorded on an audiocassette, or even whispered directly into a listener's ear. Nor are particular mediums categorically excluded from privilege protection. The relational and topical requirements common to most privileges can be satisfied in any medium, from paper to audiocassettes to whispers to the internet, so long as the element of a reasonable expectation of confidentiality is met.[438] Privileging the internet would thus create a radical, outlier privilege.

To be sure, some outliers are defensible. Perhaps a privilege for the internet could be justified despite its novelty. Privilege law has developed sensitive guidelines to help make just such a determination. For instance, in Justice Frankfurter's oft-quoted formulation, privilege is permissible "only to the very limited extent that permitting a refusal to testify or excluding relevant evidence has a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth."[439] Particularly influential is Wigmore's test, which requires: (1) privileged information must have originated in confidence; (2) confidentiality must be essential to the relationship between communicants; (3) the relationship must be valuable to society; and (4) the injury to the relationship from compelling disclosure "must be greater than the benefit thereby gained for the correct disposal of litigation."[440] More recently, in *Jaffee v. Redmond*,[441] the Supreme Court emphasized that an "[e]xception[] from the general rule disfavoring testimonial privileges may be justified"[442] when the proposed privilege "promotes sufficiently important interests to outweigh the need for probative evidence."[443] The Supreme Court elaborated factors for courts to consider in conducting that balancing, including whether a proposed privilege was "recommended by the Advisory Committee" to the FRE,[444] has been widely

---

438 *See* 23A GRAHAM & MURPHY, *supra* note 144, § 5460 n.1.
439 Elkins v. United States, 364 U.S. 206, 234 (1960) (Frankfurter, J., dissenting).
440 WIGMORE, *supra* note 215, § 2285 (emphasis omitted).
441 518 U.S. 1 (1996).
442 *Id.* at 9.
443 *Id.* (quoting Trammel v. United States, 445 U.S. 40, 51 (1980)).
444 *Id.* at 14.

adopted in state courts,[445] is "rooted in the imperative need for confidence and trust,"[446] "serves important private interests,"[447] and "serves the public interest,"[448] as well as "the likely evidentiary benefit that would result from the denial of the privilege."[449]

Consider how the Wigmore test would apply to a proposed internet privilege. To satisfy Wigmore's first prong, "[t]he communications must originate in a *confidence* that they will not be disclosed,"[450] one would have to conclude that individuals who use the internet anticipate that the communications they transmit through that medium will not be shared with others. That is almost certainly the case for a narrow set of online communications, for instance, emails between attorneys and their clients. But attorney-client communications are already protected by privilege, regardless of the medium through which they are transmitted.[451] And a wide set of online communications almost certainly do not originate in confidence, such as social media posts accessible to a large number of friends or followers. Wigmore's first prong thus counsels against creating a novel privilege for the internet.

The second prong, that "[t]his element of *confidentiality must be essential* to the full and satisfactory maintenance of the relation between the parties,"[452] depends on how the relation is defined. If the relation is that between the original sender and ultimate recipient of a message, then the same conclusion applies as applied to the first prong; confidentiality is likely essential to the relationship between some, but not most, people who use the internet to communicate. If the relation is instead that between technology companies in general and account holders in general, it becomes more complex to argue that confidentiality is essential for the maintenance of the relationship. Law enforcement can already compel technology companies to disclose the same communications contents.[453] And many technology companies themselves so far use the communications for privacy-invasive data-mining business practices.[454] Since the "relation" between technology companies and their account holders has flourished despite these significant gaps in confidentiality protections, it remains to be determined how one would claim

---

445 *Id.* at 12.
446 *Id.* at 10 (quoting *Trammel*, 445 U.S. at 51).
447 *Id.* at 11.
448 *Id.*
449 *Id.*
450 WIGMORE, *supra* note 215, § 2285.
451 *See* Conroy, *supra* note 215, at 1825.
452 WIGMORE, *supra* note 215, § 2285.
453 *See* 18 U.S.C. § 2703.
454 *See supra* p. 2783.

that confidentiality is essential for technology companies to maintain their user base.

The third prong of Wigmore's test requires that "[t]he *relation* . . . be one which in the opinion of the community ought to be sedulously *fostered*."[455] This prong again depends on how the relation is defined. If it is between the original sender and ultimate recipient of a message, then the prong is likely satisfied by some, but not most, people who use the internet to communicate. As to the relation between technology companies and their account holders, policymakers could certainly decide that it should be fostered, for instance, to encourage widespread use of the technology.[456] Importantly, though, this relationship, and the extent to which confidentiality may play a role in it, is distinct in significant ways from the kinds of relationships protected by classic professional privileges. Lawyers and clergy may depend on confidentiality to provide a service but, unlike technology companies, they do not simultaneously profit by selling or monetizing information about those who use their services.[457] In contrast, technology companies have divided loyalties between their unpaid account holders and their paying customers — other companies that purchase products and services made from mining account-holder data.[458] That distinction should give pause to policymakers contemplating extending professional privilege protections to "sedulously foster[]" technology companies.

Wigmore's fourth prong commands that, for a justified privilege, "[t]he *injury* that would inure to the relation by the disclosure of the communications must be *greater than the benefit* thereby gained for the correct disposal of litigation."[459] Congress and the courts have thus far decided that the injuries wrought on a vast array of important relations by compelling disclosures of, for instance, intimate communications between parents, children, lovers, and friends, do not rise to the level necessary to satisfy this test.[460] It is challenging to see any reason why technology companies should receive greater consideration. In total, then, the first Wigmore prong counsels clearly against a novel internet privilege, while the other three prongs offer ambiguous to no support for such a privilege.

---

455 WIGMORE, *supra* note 215, § 2285.

456 *Cf.* O'Grady v. Superior Ct., 44 Cal. Rptr. 3d 72, 87 (Ct. App. 2006) (positing that Congress enacted the SCA "to encourage 'innovative forms' of communication" (quoting S. REP. NO. 99-541, at 5 (1986))).

457 *Cf. supra* note 392 (collecting sources contemplating fiduciary duties of technology companies).

458 *See* sources cited *supra* notes 405–408 and accompanying text.

459 WIGMORE, *supra* note 215, § 2285.

460 *See, e.g.*, *In re* Grand Jury, 103 F.3d 1140, 1142 (3d Cir. 1997) (declining to recognize a parent-child privilege).

If courts, rather than Congress, were to contemplate recognizing a novel privilege for the internet, a similar analysis would apply with one key difference; courts must specifically consider the factors that *Jaffee* identified to guide their balancing of the competing interests.[461] At least two of those factors point squarely against privileging the internet. No analogous medium privilege was "recommended by the Advisory Committee" to the FRE.[462] And the majority of state courts have yet to weigh in on the issue.[463] Judges evaluating the next three *Jaffee* factors — whether such a privilege is "rooted in the imperative need for confidence and trust,"[464] and would serve both "important private interests," and "the public interest"[465] — may apply a similar analysis to that under the Wigmore factors, which weighs against the privilege. Finally, *Jaffee* instructs courts to consider "the likely evidentiary benefit that would result from the denial of the privilege."[466] Here, that benefit would be the production of otherwise unattainable, relevant, exculpatory evidence in criminal cases — an important result that would serve the interests of prosecutors, defendants, and the public alike in the truth-seeking process of the courts.

To synthesize these arguments, privilege law and theory provide vanishingly little support for, and substantial reasons to oppose, a novel evidentiary privilege for the internet. If Congress or the courts wish to create an internet privilege anyway, they should minimize the damage to the truth-seeking process of adjudication by adopting a qualified privilege. Qualified privileges can generally be defeated by balancing the litigant's interest in accessing the information against the conflicting interests that the privilege would protect on a case-by-case basis.[467] In contrast, the unqualified SCA privilege in current case law categorically suppresses relevant evidence even when it implicates no privacy interest and could exonerate the wrongfully accused.

---

461 *See supra* pp. 2788–89.

462 Jaffee v. Redmond, 518 U.S. 1, 14 (1996). Indeed, the FRE renounce any involvement in the creation of novel privileges under Rule 501. *See* FED. R. EVID. 501.

463 *See Jaffee*, 518 U.S. at 14 n.13. To date, just three state high courts have weighed in. *See* Facebook, Inc. v. Superior Ct. (*Hunter*), 417 P.3d 725, 728 (Cal. 2018); Facebook, Inc. v. Wint, 199 A.3d 625, 628–29 (D.C. 2019); State v. Bray, 422 P.3d 250, 256 (Or. 2018).

464 *Jaffee*, 518 U.S. at 10 (quoting Trammel v. United States, 445 U.S. 40, 51 (1980)).

465 *Id.* at 11.

466 *Id.*

467 *See* IMWINKELRIED, *supra* note 160, § 7.1. Crucially, qualified privileges can be defeated by a showing of need that is less than a constitutionally protected need. *See id.*

## CONCLUSION

This Article has argued against current case law that construes SCA section 2702 to bar criminal defendants from subpoenaing technology companies for the contents of another's online communications. Construing the statute this way creates an erroneous evidentiary privilege for the internet that violates the strict construction rule for statutory privileges. Correcting the case law and properly enforcing criminal defense subpoenas would further judicial truth-seeking and fairness in criminal proceedings with minimal harm to privacy. As the Supreme Court recently affirmed, "no citizen, not even the President, is categorically above the common duty to produce evidence when called upon in a criminal proceeding."[468] Technology companies should not escape that duty either.

More generally, this Article takes a first step toward illuminating the complex and surprisingly understudied relationship between the law of privacy and that of privilege. Doing so has opened a series of inquiries that are ripe for further scholarly contribution and litigation. While the focus of this Article has been the SCA and criminal defense subpoenas, the arguments developed here carry important implications for both civil subpoenas and other information privacy statutes beyond the SCA.[469] This Article has also contributed a partial definition of evidentiary privileges — namely, that a rule that bars an ex ante category of information from judicial process suffices to create a privilege — and developed a framework for properly applying the rules that govern statutory privilege construction. Future scholarship is needed to develop a more comprehensive definition of evidentiary privileges and more thoroughly analyze the *St. Regis* strict construction canon for statutory privileges. This definition and framework should help to resolve future conflicts between information privacy and truth-seeking in the courts.

Finally, this Article has identified a federal circuit split as to a) whether federal statutes must contain express privilege language before courts may decide that Congress intended the statute to create an

---

[468] Trump v. Vance, 140 S. Ct. 2412, 2431 (2020).

[469] *See generally* Wexler, *supra* note 52 (documenting multiple privacy statutes that contain express exceptions for law enforcement investigators but silence as to criminal defense subpoenas). Notably, those implications are also cabined. Because the arguments developed here are statutory, they do not affect potential Fourth Amendment restrictions on subpoenas seeking electronic communications contents or other sensitive evidence.

evidentiary privilege that abrogates the legislated subpoena and discovery rules and impedes judicial truth-seeking; or b) whether courts may read ambiguous silence in statutory text to impliedly create such a privilege. Supreme Court guidance is needed to resolve that question.