ARTICLE

FOURTH AMENDMENT NOTICE IN THE CLOUD

JESSE LIEBERFELD* **& NEIL RICHARDS****

ABSTRACT

The widespread storage of documents through the range of Internet technologies known as "the cloud" offers tremendous convenience but also creates significant risks of exposure to third parties. In particular, law enforcement investigators seeking access to potentially relevant evidence have aggressively and extensively used the Electronic Communications Privacy Act of 1986 ("ECPA") to execute digital searches. But a relatively obscure provision of ECPA, § 2703, allows law enforcement to search a person's Fourth Amendment "papers" without them ever learning that a warrant has allowed the exposure of their private, sensitive, and possibly incriminating documents. What is more, federal and state law enforcers use their § 2703 secret search power many thousands of times per year, mostly on individuals that they will likely never charge with crimes. This practice denies countless cloud users their traditional Fourth Amendment right to notice of a search.

This Article examines the problem of unannounced searches in the cloud and the legal and technological frameworks in which those searches operate. By analyzing the problem through the frames of communications privacy, constitutional history, and Fourth Amendment doctrine, the Article concludes that the current practice of unannounced searches under ECPA fails to meet the basic notice requirement of the Fourth Amendment—a foundational civil liberty that is ancient, important, and hard-won, but also difficult to vindicate through litigation. The Article first explains the ancient origins of the right of notice and how it is threatened by the current federal statutory framework for digital searches. At the policy level, it then identifies the elements that must be

* Microsoft Cloud Civil Liberties Fellow, Cordell Institute, Washington University.

** Koch Distinguished Professor in Law; Director, Cordell Institute, Washington University. The authors thank Hasan Ali, Norm Barbosa, Sue Glueck, and David Pendle for their insights into the consequences of warrants issued without notice; Travis Crum, Danielle D'Onfro, Dan Epps, Patricia Hageman, Jonathan Heusel, Peter Joy, and participants at the Washington University Cordell Institute Ideas Lunch and the Privacy Law Scholars Conference for their feedback; Sara Hubaishi for researching and compiling transparency reports; Gary Liu for cite-checking; and Michael Washington for his meticulous research on the historical origins of the principle of notice accompanying government searches.

incorporated into long-overdue reforms to federal electronic surveillance law to comply with basic norms of the Fourth Amendment.

CONTENTS

INTRODUCTION

Today, we store much of our personal information using internet-based hardware and software services—a technology and business model known as "cloud computing."[1] Cloud computing allows people to access stored information from any physical location with an internet connection, provides near-unlimited storage, and enables large groups to collaborate on projects.[2] As a result, the practice has become an inescapable part of modern life, provided by a range of companies familiar to virtually every consumer, whether Apple iCloud, Amazon Web Services, Box, Dropbox, Google Cloud, Microsoft OneDrive, or many others. Cloud computing, for example, was used to draft and edit this Article, and you may well be using "the cloud" to read it now.

Cloud computing is convenient, but, like many digital conveniences, it also carries real risks of exposure and harm. Most significantly, storing documents in the cloud heightens the risk that those documents might be accessed by third parties, particularly law enforcement. The Supreme Court has recognized that cloud computing has become an essential element of modern life,[3] but the technology also requires us to entrust our sensitive information to large tech companies whose interests may differ from our own.[4] Perhaps recognizing this fact, as well as the exponentially increasing amount and sensitivity of cloud-stored data, law enforcement authorities have eagerly sought such data from cloud service providers. The volume of such requests can be startling to the uninitiated. For example, Google received over 97,000 such requests in the United States in 2021 alone and disclosed customer data to law enforcement in over 80% of these cases.[5]

State and federal law enforcement have sought most of these orders to cloud companies to allow government access under the Electronic Communications Privacy Act of 1986 ("ECPA")..[6] Though it is ancient in terms of Internet Time

---

[1] Eric Griffith, *What Is Cloud Computing?*, PCMAG (Feb. 15, 2022), https://www.pcmag.com/news/what-is-cloud-computing [https://perma.cc/4D33-UDQW].

[2] Chris Preimesberger, *Cloud Computing Pros and Cons: The Good, the Bad, and the Gray Areas*, ZDNET (Sept. 20, 2021), https://www.zdnet.com/article/cloud-computing-pros-and-cons/ [https://perma.cc/UQQ3-23C9].

[3] *See* Riley v. California, 573 U.S. 373, 385, 397-98 (2014).

[4] For a more general overview of some of the problems of trust in the cloud and other digital contexts, see, for example, Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 1004 (2021); Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1712-16 (2020); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1219-23 (2017); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 435 (2016); Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985, 986-92 (2022).

[5] *Global Requests for User Information*, GOOGLE TRANSPARENCY REP., https://transparencyreport.google.com/user-data/overview (last visited Apr. 18, 2023).

[6] *See, e.g.*, *United States Legal Process FAQs*, TRANSPARENCY REP. HELP CTR., https://support.google.com/transparencyreport/answer/9700059 [https://perma.cc/9RDM-BSZV] (last visited Apr. 18, 2023); *About Apple's Transparency Report*, APPLE,

and outdated in many ways, ECPA is nonetheless the primary statute governing law enforcement access to cloud data. From a law enforcement perspective, ECPA is a dream. The trove of potentially incriminating evidence available on the cloud presents the opportunity to search through vast swathes of citizens' personal information with the added benefit of secrecy. After all, while it's hard not to notice when a SWAT team executing a search warrant breaks down your front door, the nature of cloud technology is such that their colleagues in digital investigations can secretly comb through your cloud files for years without your ever noticing. Most of these secret ECPA searches target individuals who will likely never be charged with a crime.[7]

Secret ECPA searches of this sort are authorized by § 2703 of ECPA.[8] This section's provisions allow law enforcement to search the contents[9] of much of our everyday communication "without required notice to the subscriber or customer, if the governmental entity obtains a warrant."[10] As such, it brings into reality Justice Louis Brandeis's fear from nearly a century ago that

> [w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, . . . expos[ing] to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.[11]

Brandeis's uncanny prophecy nicely illustrates some of § 2703's Fourth Amendment implications, but secret government searches have First Amendment implications as well. As Jonathan Witmer-Rich observes, "[w]hen a government conducts covert searches of its own citizens, and citizens begin to learn of that practice, . . . [e]ach person in the community, regardless of whether they have been targeted or not, suffers the uncertainty of not knowing whether the government has violated their privacy."[12] Witmer-Rich notes that this is

https://www.apple.com/legal/transparency/about.html [https://perma.cc/3D7S-NGWH] (last visited Apr. 18, 2023); *Government Requests for User Data: United States*, META, https://transparency.fb.com/data/government-data-requests/country/US/ [https://perma.cc/DD96-AAGE] (last visited Apr. 18, 2023).

[7] *See* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 328 n.83 (2012) (noting "DOJ produced a list of only 255 criminal prosecutions over a period of approximately seven years after September 11, 2001" in response to a FOIA request for "docket information for any case in which an individual was prosecuted after the government obtained an order for cell phone location data without a showing of probable cause").

[8] 18 U.S.C. § 2703.

[9] Under ECPA, "'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." *Id.* § 2510(8).

[10] *Id.* § 2703(b)(1)(A).

[11] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[12] Jonathan Witmer-Rich, *The Fatal Flaws of the "Sneak and Peek" Statute and How To Fix It*, 65 CASE W. RES. L. REV. 121, 130 (2014). Although Witmer-Rich primarily addresses

"precisely why covert searching and surveillance are tools exploited by totalitarian regimes. The practice of covert searching is dangerous, especially if conducted frequently and with lengthy delays in notice, and must therefore be subjected to exacting constitutional scrutiny that has been largely absent in judicial decisions to date."[13]

This Article makes a simple but significant claim: Unannounced searches under § 2703 as it is currently drafted violate the Fourth Amendment, and they do so in ways that cut to the core of the reason why we have protections against unreasonable searches and seizures in the first place.[14] Courts have understood for hundreds of years that both the Fourth Amendment and the common law from which it originated require that law enforcement officials announce their presence before conducting searches.[15] Originally, this rule was understood to have no exceptions, both in England[16] and the United States.[17] Courts traditionally saw this inflexible rule as necessary to preserve both property rights and the presumption of innocence, assuming that an occupant who knew of an officer's lawful authority would obey the officer's commands.[18] In modern times, courts have allowed authorities more leeway, reinterpreting this requirement as one of several factors in determining whether a search was properly executed.[19] However, none of the rationales for this jurisprudential shift apply to secret searches in the digital realm: Courts' justifications for this shift have largely focused on avoiding potential violence against officers, destruction

unannounced searches of physical property, the same privacy concerns exist in digital spaces where many of our most personal communications are stored.

[13] Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches, and the Fourth Amendment "Rule Requiring Notice,"* 41 PEPP. L. REV. 509, 585 (2014) (footnote omitted); *see also* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 4-5 (2015).

[14] U.S. CONST. amend. IV. The specific ECPA provisions at issue are 18 U.S.C. § 2703(a)-(b)(1)(B). There are also valid Fourth Amendment concerns regarding the use of court orders to obtain communications at a lower evidentiary threshold than probable cause, as § 2703(d) authorizes. This Article focuses on the provisions requiring warrants to demonstrate that even obtaining a warrant does not itself satisfy the Fourth Amendment's requirements.

[15] *See infra* Part II.

[16] *See, e.g.*, Semayne's Case (1604) 77 Eng. Rep. 194, 195-96 (KB); Foster v. Hill (1611) 80 Eng. Rep. 839, 839 (KB); Cook's Case (1640) 79 Eng. Rep. 1063, 1063; 3 WILLIAM BLACKSTONE, COMMENTARIES *412 ("[T]he sheriff . . . may justify breaking open doors, if the possession be not quietly delivered."); SIR EDWARD COKE, 4 INSTITUTES OF THE LAWS OF ENGLAND 177 (London, W. Clarke & Sons 1817) (1644) ("[I]f one be indicted of felony, the sheriff may by process thereupon after denyall made, &c. break the house . . . ."); SIR MATTHEW HALE, 2 HISTORY OF THE PLEAS OF THE CROWN 151 (Solemn Emlyn ed., 1736).

[17] *See, e.g.*, Kelsy v. Wright, 1 Root 83, 84 (Conn. 1783); Oystead v. Shed, 13 Mass. (12 Tyng) 520, 523 (1816); Haggerty v. Wilber, 16 Johns. 287, 288-89 (N.Y. Sup. Ct. 1819); Burton v. Wilkinson, 18 Vt. 186, 189-90 (1846); Barnard v. Bartlett, 64 Mass. (10 Cush.) 501, 502-03 (1852); Commonwealth v. Reynolds, 120 Mass. 190, 197 (1876).

[18] *See, e.g.*, *Semayne's Case*, 77 Eng. Rep. at 195-96.

[19] *See, e.g.*, Richards v. Wisconsin, 520 U.S. 385, 394 (1997); Wilson v. Arkansas, 514 U.S. 927, 934 (1995).

of evidence, or a suspect's escape. Where such dangers are present, courts have allowed searches without notice.[20] However, when electronic communications are searched, there is no occupant to retaliate against officers, destroy evidence, or escape. Thus, in the digital sphere, we have the problem of unprecedented levels of digital surveillance in a context where the traditional justifications for secret searches are absent.

The notice principle has deep roots in our law, and if courts were to take this principle seriously, § 2703 searches as currently executed simply could not meet the Fourth Amendment's warrant requirement. In fact, the logical implications of recent Supreme Court and circuit court rulings already point towards this result. In 2010, when the government sought to use ECPA to obtain 27,000 of a suspect's emails without obtaining a warrant, the Sixth Circuit held in *United States v. Warshak*[21] that the order constituted a search subject to the Fourth Amendment warrant requirement.[22] Four years later, the Supreme Court held in *Riley v. California*[23] that the only exceptions to the warrant requirement potentially relevant to such searches—those based on "harm to officers and destruction of evidence"—did not apply to digitally stored information.[24] In the 2018 case of *Carpenter v. United States*,[25] the Court tacitly affirmed *Warshak*'s central holding[26] and specifically applied *Riley* to electronic evidence governed by ECPA.[27] It follows quite logically from these premises that § 2703 searches for incriminating evidence are governed by the Fourth Amendment, and that they are unconstitutional absent a properly executed warrant.[28] To properly execute a warrant, law enforcement must either notify the suspect or show that the notice requirement is waivable.[29] Therefore, unannounced § 2703 searches are unconstitutional if courts treat the notice requirement as an inflexible element of the warrant requirement. And even if there were to be some

[20] *See, e.g.*, *Richards*, 520 U.S. at 395-96; *Wilson*, 514 U.S. at 937.

[21] 631 F.3d 266 (6th Cir. 2010).

[22] *Id.* at 288 ("[T]o the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."). The Fourth Amendment warrant requirement should not be confused with the statutory warrant requirements to invoke 18 U.S.C. § 2703(a)-(b)(1)(B). It is a claim of this Article that while the statutory regime is complex, the basic principles of civil liberties at stake are quite simple.

[23] 573 U.S. 373 (2014).

[24] *Id.* at 386.

[25] 138 S. Ct. 2206 (2018).

[26] *Id.* at 2222 (describing as "sensible" principle that the warrant requirement should apply anytime "Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party").

[27] *Id.* (using Court's precedent holding search of cell phone information "bears little resemblance" to brief physical searches to support conclusion that "Court has been careful not to uncritically extend existing precedents" when "confronting new concerns wrought by digital technology" (citing *Riley*, 573 U.S. at 386)).

[28] *See, e.g.*, *Carpenter*, 138 S. Ct. at 2221.

[29] *See, e.g.*, Wilson v. Arkansas, 514 U.S. 927, 934 (1995); Richards v. Wisconsin, 520 U.S. 385, 394 (1997).

flexibility, the vast bulk of the many secret searches routinely conducted under ECPA would nonetheless be unconstitutional.

Compounding this problem, ECPA's notice problems have another, more sinister dimension. In addition to using § 2703 to search without telling the suspect (or person suspected of having evidence relevant to an investigation), there is a separate provision of ECPA that allows so-called "preclusion-of-notice orders."[30] This provision, § 2705(b), lets the government place a gag order on cloud companies, preventing them from informing their customers of the search.[31] Though perhaps intended by the drafters of ECPA to be used occasionally, in practice the provision has been abused by law enforcement, allowing them to "restrain[] the provider indefinitely from notifying the subscriber."[32] This provision creates logistical problems for any plaintiff wishing to challenge such warrants' constitutional validity. First, cloud service providers know when the warrants are issued, but lack standing to challenge them. Second, while subscribers have standing to challenge the warrants, they frequently cannot be informed of their existence. Third, the government knows, but it's not telling under § 2703.

Both cloud storage providers and civil rights groups have challenged law enforcement's ability to withhold notice, most notably in the case of *Microsoft Corp. v. U.S. Dep't of Just.*[33] In 2016, after being consistently subjected to large numbers of these warrants, Microsoft challenged the warrants on Fourth Amendment grounds and the preclusion-of-notice orders on First Amendment grounds, arguing that they represented an unconstitutional prior restraint on freedom of speech.[34] Many other large cloud storage providers, including Amazon, Apple, Dropbox, Google, and Salesforce supported Microsoft's position.[35] The U.S. District Court for the Western District of Washington found that Microsoft had "adequately alleged a facially plausible First Amendment claim"[36] and "adequately support[ed its] claim that Section 2705(b) [the preclusion-of-notice order provision] is unconstitutionally overbroad,"[37] but Microsoft dropped the case when the Department of Justice revised its policy on preclusion-of-notice orders, granting companies greater leeway to inform consumers of searches targeting their accounts.[38] Notably, however, the court

[30] *In re* Application of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2705(b), 131 F. Supp. 3d 1266, 1267 (D. Utah 2015).

[31] 18 U.S.C. § 2705(b).

[32] *In re* Application of the U.S. for an Ord. Pursuant to 18 U.S.C. § 2705(b), 131 F. Supp. 3d at 1271-72.

[33] 233 F. Supp. 3d 887 (W.D. Wash. 2017).

[34] *Id.* at 896-97.

[35] Cyrus Farivar, *DOJ Changes "Gag Order" Policy, Microsoft To Drop Lawsuit*, ARS TECHNICA (Oct. 24, 2017, 5:12 AM), https://arstechnica.com/tech-policy/2017/10/doj-changes-gag-order-policy-microsoft-to-drop-lawsuit/ [https://perma.cc/2LE8-H8PK].

[36] *Microsoft*, 233 F. Supp. 3d at 908.

[37] *Id.* at 910.

[38] Farivar, *supra* note 35.

dismissed Microsoft's Fourth Amendment claim, holding that Microsoft lacked standing to challenge these searches on its customers' behalf and that assessing Microsoft's theory of the Fourth Amendment was "more properly left to higher courts."[39] Consequently, the constitutionality of secret searches under § 2703 warrants remains unresolved.

Ordinarily in cases of this sort, the most straightforward remedy would be to bring a constitutional challenge against the statute. However, as the *Microsoft* case suggests, there are significant practical challenges to bringing such suits.[40] Cases based on such warrants are unlikely to reach trial because only a minority of § 2703 cases leads to prosecutions,[41] and ECPA contains no statutory provision allowing warrants to be challenged in advance.[42] Even if one of the rare targets charged with a crime were to challenge the order's constitutionality, demonstrating a Fourth Amendment violation might not result in suppression of the evidence.[43] And even if a defendant somehow managed to undertake the lengthy process of appealing the warrant, higher courts could easily resolve the decision by invalidating the *application* of § 2703 rather than striking down the offending provisions. Given these obstacles, only a legislative solution to this constitutional problem would be effective. Congress should therefore repeal the provisions of § 2703 allowing the government to withhold notice once it has obtained a warrant.

We develop our argument in four parts. Part I lays the foundation for the analysis which follows, which shows how § 2703 warrants have evolved into a tool for law enforcement to routinely access our personal information without notifying us. Reviewing the history of electronic communications surveillance over the past century, Part I shows how, before ECPA was drafted in the mid-1980s, the main threat from communications surveillance was wiretapping but that today it is now stored data. As a result, ECPA gave short shrift to the dangers of indiscriminate, secret access to stored data. This mistake enabled our current regime of large-scale secret government searches in the cloud, in which the protections ECPA intended have been turned on their head.

Part II places the problem of secret and delayed-notice searches in a broader historical context. It explains how, from the Middle Ages until the nineteenth century, the law was clear that there must be actual notice to a person before a warrant was executed to search their homes or papers, and that this rule had no exceptions. While the announcement rule was modified over the twentieth century to accommodate risks that a suspect might escape, might react violently towards an officer, or might destroy evidence, these exceptions do not apply in a digital context. Accordingly, we argue that the best reading of the

[39] *Microsoft*, 233 F. Supp. 3d at 916.

[40] *Id.*

[41] *See* Smith, *supra* note 7, at 313, 328 n.83.

[42] *See id.* at 330 n.93 (citing 18 U.S.C. § 2707(e)).

[43] *See id.* at 327 n.81 ("Even if a constitutional violation is shown, relief may be denied if the officer acted in good faith.").

announcement rule in the digital context is that it should retain its ancient, inflexible, and civil liberties-protecting character.

Part III shifts the frame of analysis from legislative and constitutional history to current legal doctrine. It explains how contemporary searches under § 2703 that do not satisfy the warrant requirement are unconstitutional. Reviewing the modern requirements for the execution of constitutionally protected searches, Part III concludes that as a matter of current doctrine, law enforcement authorities cannot use exceptions to the warrant requirement based on suspects' ability to escape, threaten officers, or destroy evidence to obtain digitally stored evidence warrantlessly. It also explains that both the specific holdings and general trend of recent Supreme Court rulings on digital searches offer additional support for the conclusion that searches without notice under § 2703, as practiced in our modern cloud-mediated context, fail to meet basic Fourth Amendment requirements.

Part IV turns to solutions. It explains that while litigation is normally our first recourse to address constitutional violations, the problem of § 2703 searches without notice defies such a straightforward solution. Because there are significant limitations facing litigants who wish to challenge § 2703, only a legislative remedy will be appropriate for this particular legislative and constitutional problem. Congress's goal, we argue, should be to provide subjects of such searches with the same presumption of innocence and property rights as the original notice requirement, including the adjoining Fourth Amendment right to be secure in one's papers and effects. To help future legislators who might wish to tackle this problem through reform, we offer a framework for developing a communications privacy statute for the age of the cloud. This framework would allow reasonable government access to relevant evidence in a way that does not compromise our long-held and essential constitutional commitments to notice of government searches. Specifically, we advocate implementing safeguards like those ECPA requires for wiretaps, which contain much more stringent restrictions on law enforcement's collection, use, and disclosure of information than traditional warrants.

I. THE BREADTH OF UNANNOUNCED CLOUD ORDERS

Before delving into history and current doctrine, it is first necessary to set the stage for the argument which follows by explaining how § 2703 warrants have evolved into a tool for law enforcement to routinely access our personal information without notifying us. Accordingly, this Part reviews the history of communications surveillance, showing that before ECPA, most invasions of privacy from communications surveillance were wiretapping abuses. Although stored communications existed when ECPA was passed, they were costly and rarely used, and even then, they largely existed only on a temporary basis.[44]

[44] *See* Lucas Mearian, *CW@50: Data Storage Goes from $1M to 2 Cents per Gigabyte (+Video)*, COMPUTERWORLD (Mar. 23, 2017, 6:00 AM), https://www.computerworld.com

There being nothing like the cloud in 1986, Congress gave stored communications surveillance much less attention than the rigorous oversight it gave wiretapping.[45] Thus, under ECPA, law enforcement authorities searching stored communications do not need to justify each use and disclosure of information, in sharp contrast to a wiretap request for which a stringently justified warrant is required.[46] Furthermore, the authorities seeking digital evidence do not operate under the same particularity requirements as they would when searching physical property. Today, when the cloud mediates our lives far more than the telephone, and when stored communications are ubiquitous but wiretapping is relatively rare, this comparative lack of oversight enables law enforcement to access much of our personal information without our knowledge.

A. *The Old Privacy Threat of Wiretapping*

ECPA governs most electronic surveillance today.[47] As Deputy U.S. Chief Technology Officer for Policy Deirdre Mulligan explains it well, ECPA "created the statutory framework of privacy protections and related standards for law enforcement access covering electronic communications and remotely stored electronic records."[48] The law regulates two types of electronic surveillance: real-time wiretaps[49] and surveillance of stored communications,[50] including the provisions allowing law enforcement to conduct unannounced searches.[51] However, as the methods of communication common in 1986 differ vastly from those commonly used today, ECPA has had consequences that could not have been anticipated when the act was passed. This Section discusses how technological shifts since 1986 have rendered § 2703 warrants a much more potent surveillance technique than they were when Congress enacted ECPA, and how they now enable law enforcement to access much of our personal information without notice. Changes in technology have thus turned a statute intended to protect privacy and other civil liberties into one that enables their secret violation at scale.

Section 2703 covers two types of services which govern much of our everyday communication. The first, an "electronic communications service," is

/article/3182207/cw50-data-storage-goes-from-1m-to-2-cents-per-gigabyte.html [https://perma.cc/34W2-3GLU] (noting one gigabyte of disk storage cost $40,000 in 1985).

[45] *See* Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT TECH. REV. (Oct. 31, 2011), https://www.technologyreview.com/2011/10/31/257406/who-coined-cloud-computing/ [https://perma.cc/FP94-TTFL].

[46] *See* 18 U.S.C. §§ 2510-2522, 3121-3127.

[47] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[48] Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557 (2004).

[49] 18 U.S.C. §§ 2510-2522, 3121-3127.

[50] *Id.* §§ 2701-2711.

[51] *Id.* §§ 2703, 2705.

defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[52] Such services include email, phone, and text messaging services, and social media platforms.[53] The second, a "remote computing service," is defined as the "provision to the public of computer storage or processing services by means of an electronic communications system."[54] This definition covers offsite storage used by businesses to house or process data.[55] Many online communications platforms provide both types of services.[56] Consequently, each of these definitions governs vast quantities of personal data.

Once law enforcement officials have obtained a warrant, § 2703 allows communications stored using either method to be searched without notice. Section 2703(b)(1)(A) allows governmental entities to require remote computing service providers to disclose contents of electronic or wire communications "without required notice to the subscriber or customer, if the governmental entity obtains a warrant."[57] For electronic communications services, § 2703(a) requires that law enforcement notify providers (but not customers) when searching communications that have been stored for up to 180 days.[58] However, if a communication "has been in electronic storage in an electronic communications system for more than one hundred and eighty days," § 2703(a) allows governmental entities to require disclosure "by the means available under subsection (b) of this section"[59]—i.e., to execute a warrant without notifying the provider or customer.[60] These provisions allow most contents of our emails, social media messages, files stored in the cloud, and other electronic communications to be searched without our knowledge.

It is unlikely that Congress intended this result. To understand the assumptions under which ECPA's drafters operated, it is necessary to first review how surveillance had developed in the years preceding the law. Among the first major threats to communications privacy was telephone wiretapping, which had become an increasingly serious problem since the telephone's

[52] *Id.* § 2510(15).

[53] *See, e.g.*, Garcia v. City of Laredo, 702 F.3d 788, 792 (5th Cir. 2012) (noting that courts have understood ECPA provisions to apply to communication service providers such as telephone companies, email service providers, and bulletin board services).

[54] 18 U.S.C. § 2711(2).

[55] *See* S. REP. NO. 99-541, at 2-3 (1986).

[56] *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982, 987. (C.D. Cal. 2010); Shenwick v. Twitter, Inc., No. 16-cv-05314, 2018 WL 833085, at *2 (N.D. Cal. Feb. 7, 2018).

[57] 18 U.S.C. § 2703(b)(1)(A).

[58] *Id.* § 2703(a).

[59] *Id.*

[60] *Id.* § 2703(b)(A).

invention a century earlier.[61] In the 1928 case *Olmstead v. United States*,[62] a defendant challenged the practice as violating his rights under the Fourth Amendment. The Supreme Court, however, held that wiretapping "did not amount to a search or seizure within the meaning of the Fourth Amendment."[63] The Court reasoned that no defendant's Fourth Amendment rights were violated "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[64]

The task of regulating communications surveillance thus fell to Congress, and early federal communications surveillance laws primarily regulated wiretaps. The earliest of these was the Communications Act of 1934,[65] which stated that "no person not being authorized by the sender shall intercept any radio communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[66] While this act applied to law enforcement as well as private citizens, it only prohibited officials from *disclosing* intercepted communications, not from engaging in wiretapping itself.[67]

In 1967, two key Supreme Court decisions changed the landscape of communications law. *Katz v. United States*[68] overruled *Olmstead*, holding that "a person in a telephone booth may rely upon the protection of the Fourth Amendment" against warrantless electronic monitoring by law enforcement, even when "the surveillance technique they employed involved no physical penetration of the telephone booth."[69] More generally, *Katz* repudiated *Olmstead*'s holding that only acts of trespass could constitute searches, instead holding that "the Fourth Amendment protects people, not places."[70] After *Katz*, law enforcement officials could no longer disregard the Fourth Amendment simply because they never actually entered a defendant's property.

The same year, the Court held in *Berger v. New York*[71] that a state law authorizing wiretapping without procedural safeguards was unconstitutional.[72] In light of these developments, Congress updated federal communications

[61] *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 378-79, 378 n.18 (2014).

[62] 277 U.S. 438 (1928).

[63] *Id.* at 466.

[64] *Id.*

[65] Pub. L. No. 73-416, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151-615b (2006)).

[66] *Id.*

[67] *See* Nardone v. United States, 308 U.S. 338, 341 (1939).

[68] 389 U.S. 347 (1967).

[69] *Id.* at 352.

[70] *Id.* at 351.

[71] 388 U.S. 41 (1967).

[72] *See id.* at 60 (holding "statute's blanket grant of permission to eavesdrop is without adequate judicial supervision or protective procedures").

surveillance law with the Wiretap Act of 1968.[73] In an attempt to fulfill *Berger*'s requirements, the Wiretap Act imposed several key restrictions on law enforcement's use of wiretapping. Specifically, the Act required agents to obtain a warrant by showing special need, a predicate felony offense, and Department of Justice or high-level state approval before wiretapping a phone call.[74] The Act required law enforcement to provide the authorizing judge with "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous" in support of this showing.[75] Additionally, the Act required officers to "minimize the interception of communications not otherwise subject to interception,"[76] and to not disclose the information they intercept unless it "is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure."[77] In other words, agents must minimize the interception of communications and justify each use and disclosure of information they intercepted.[78]

In 1968, Congress was still largely regulating technologies whose primary privacy vulnerability was real-time wiretapping.[79] However, technologies allowing communications to be preserved and reviewed later on were already emerging, and no federal statute governed law enforcement officers' ability to acquire and use them. For instance, the Fifth Circuit held in *United States v. Turk*,[80] that the Wiretap Act did not apply to officers seeking to replay a cassette tape seized from a defendant's car.[81] As Professor Orin Kerr documents, "[b]y the mid-1980s, Congress grew concerned about new computer telecommunications methods that fell outside the scope of existing privacy laws."[82] A 1985 Office of Technology Assessment report documented the increasing prevalence of communication via computers, specifically "electronic mail" (meaning content that could be sent between computers over telephone

[73] 18 U.S.C. § 2511.

[74] *See id.* §§ 2516, 2518 (enumerating conditions under which federal and state governments will authorize wiretaps and application process for wiretap authorization, but also carving out emergency situations permitting agents to wiretap before receiving authorization).

[75] *Id.* § 2518(1)(c).

[76] *Id.* § 2518(5).

[77] *Id.* 802 § 2517(1).

[78] *See* United States v. Hall, 543 F.2d 1229, 1233 (9th Cir. 1976) (interpreting 18 U.S.C. § 2517(1) as "designed to protect the public from unnecessarily widespread dissemination of the contents of interceptions and from the wholesale use of information gleaned from a legal wiretap by an officer—state or federal—for personal or illegal purposes").

[79] *See* 18 U.S.C. § 2511.

[80] 526 F.2d 654 (5th Cir. 1976).

[81] *See id.* at 670.

[82] Kerr, *supra* note 61, at 380.

lines and printed in hard copy),[83] which exceeded the Wiretap Act's scope. However, as Mulligan observes, "the OTA report did not consider, or make recommendations on, the remote storage of electronic records on third-party servers generally. Instead, it covered only electronic mail."[84]

With the Wiretap Act increasingly failing to keep pace with technology, Congress enacted ECPA in 1986.[85] Mulligan notes that "ECPA was both a proactive and reactive statute."[86] It was designed to both "provide a predictable privacy framework, spurred by the recognition that individuals would be reluctant to use new technologies unless privacy protections were in place" and "head off the possibility of courts concluding that the Fourth Amendment did not protect electronic communications and electronic records on third-party servers."[87] ECPA consists of three titles. Two of these titles regulate real-time wiretaps: One amended the Wiretap Act and extended its protections to computer transmissions,[88] while another, the Pen Register Statute,[89] prohibited the use of pen registers or tap-and-trace technologies to record electronic communications without a court order.[90] The remaining piece, the Stored Communications Act ("SCA"),[91] regulates access to stored records.[92] The provisions enabling searches without notification[93] and preclusion-of-notice orders[94] are part of this title.

These measures largely achieved ECPA's reactive aim: They secured some oversight for surveillance of computers, and courts have since held that many forms of electronic communication merit Fourth Amendment protection.[95] However, the statute's proactive aim has not fared as well—the SCA does not yield a robust, predictable privacy framework, and much of our current personal information is now governed by it. The next Section discusses this development.

---

[83] *See* OFF. OF TECH. ASSESSMENT, OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 3-4, 47 (1985).

[84] Mulligan, *supra* note 48, at 1564 (footnote omitted).

[85] *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[86] Mulligan, *supra* note 48, at 1565.

[87] *Id.*

[88] *See* 18 U.S.C. §§ 2510-21.

[89] *Id.* §§ 3121-3124, 3126-3127.

[90] *See id.*; *see, e.g.*, *In re* Ord. Authorizing Installation of Pen Reg., 846 F. Supp. 1555, 1558-61 (M.D. Fla. 1994).

[91] 18 U.S.C. §§ 2701-2712.

[92] *See id.* §§ 2701-2709, 2711.

[93] *See id.* § 2703(a)-(b)(1)(B).

[94] *See id.* § 2705(b).

[95] *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (holding "Government's acquisition of [Carpenter's] cell-site records was a [Fourth Amendment] search"); United States v. Warshak, 631 F.3d 266, 284 (6th Cir. 2010) (holding that "contents of [defendants'] emails" merited Fourth Amendment protection). Both cases concerned orders issued under ECPA.

B. *The Current Privacy Threat of Stored Communications*

When ECPA was passed, Congress likely did not anticipate that its application to today's technology would give law enforcement such a powerful tool. At the time, remote storage was extremely rare. ECPA covers two types of communications—real-time wiretaps[96] and stored communications like those at issue in *Microsoft*.[97] Today, the latter are far more ubiquitous than the former.[98] But in 1986, stored communications played a secondary role in information sharing, because data was almost inconceivably more expensive and difficult to store than today. For example, a single gigabyte of disk drive storage space cost about $40,000 the year prior to ECPA's enactment.[99] By 2017, the cost of storage per gigabyte had dropped to approximately $0.02.[100] Given the high costs of storage around the time of ECPA's passage, most service providers and consumers sought to minimize their stored communications.[101] Accordingly, most information was then stored on third-party servers for very short intervals, until it could be transferred to a personal computer.[102] Because it is far more practical today for subscribers to store most of their files, emails, and other communications online indefinitely, the SCA is invoked far more frequently and applies to a much broader array of content than its drafters could have envisioned.[103] Accordingly, § 2703 has far more expansive scope in practice today than when it was enacted. Moreover, it now applies to information that users might reasonably expect to store and keep private for extended intervals. Thus, § 2703 now enables law enforcement to access much of citizens' personal information without their knowledge.

The SCA's protections against excessive surveillance were far less stringent than those in the Wiretap Act. Notably, it omitted the Wiretap Act's requirements that agents minimize the interception of communications[104] and justify each use and disclosure.[105] Whereas these Wiretap Act provisions transcended typical warrant requirements, the SCA lacked these extra safeguards, often granting greater latitude than is typical of warrants. In contrast to the Wiretap Act, the SCA allows law enforcement to access entire user accounts.[106] As Kerr notes, "The government is then free to look through all of

[96] 18 U.S.C. § 2510.

[97] *Id.* §§ 2701-11; Microsoft Corp. v. U.S. DOJ, 233 F. Supp. 3d 887, 894-97 (W.D. Wash. 2017).

[98] *See* Kerr, *supra* note 61, at 391.

[99] Mearian, *supra* note 44.

[100] *Id.*

[101] *See* Kerr, *supra* note 61, at 391.

[102] *See* OFF. OF TECH. ASSESSMENT, *supra* note 83, at 47.

[103] *See* 18 U.S.C. §§ 2701-13.

[104] *See* Kerr, *supra* note 61, at 384; Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1298 (2004).

[105] *See* 18 U.S.C. §§ 2702-2703.

[106] *Id.* § 2703(b)(2).

it, with no limits on the government's power to use communications it finds, whether relevant or not to the crime under investigation."[107] Likewise, Kerr explains that, unlike the Fourth Amendment, the SCA "imposes no limits on particularity: there is no need to be specific as to which emails, which files, or which records were obtained. Instead, disclosure of one record allows disclosure of all records."[108] Combined with the SCA's leniency on use, disclosure, minimization, and particularity, § 2703 gave law enforcement great latitude in searching stored communications without the owner's knowledge.

As Kerr observes, Congress may have given wiretaps greater protection than stored communications because they were more prevalent at the time.[109] However, technological advances have reversed this dynamic. As we have seen, when ECPA was passed, large-scale remote computer storage was prohibitively expensive,[110] incentivizing most consumers and businesses to store communications only until they could be moved to personal computers.[111] Today, when a standard free Google Drive account comes with fifteen gigabytes of storage[112] (potentially worth at least $600,000 in 1985), stored communications are far more ubiquitous, and consumers have virtually no need to delete any communication. Storage has gone from being prohibitively expensive to practically free. Furthermore, many providers' business models today depend explicitly on preserving and aggregating mass quantities of their users' stored communications, as this allows them to earn revenue through targeted advertising.[113] The result is that today, the government can search most of our electronic communications without notifying us, a consequence Congress likely did not intend.

In light of these developments, the relative frequencies of law enforcement requests for real-time wiretaps and stored communications have inverted. According to Google's most recent transparency report, it received 30,030 search warrants for its users' accounts between January and June 2022, but received no wiretap orders during that time.[114] Since Google first began sorting

[107] Kerr, *supra* note 61, at 384.

[108] *Id.* at 383-84.

[109] *See id.* at 391-94.

[110] Mearian, *supra* note 44.

[111] OFF. OF TECH. ASSESSMENT, *supra* note 83, at 47.

[112] *Review Storage Use Across Your Organization: Storage Management Tool FAQs*, GOOGLE WORKSPACE ADMIN HELP, https://support.google.com/a/answer/12002268 [https://perma.cc/J46P-2WNS] (last visited Apr. 18, 2023) (reporting user with "Essentials Starter" edition has fifteen gigabytes of storage per user).

[113] *See, e.g.*, ROBERT SHAPIRO & SIDDHARTHA ANEJA, WHO OWNS AMERICANS' PERSONAL DATA, AND WHAT IS IT WORTH? 11 (2020), https://assets.futuremajority.org/uploads/report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-2019.pdf [https://perma.cc/U93X-J92X] (finding Google earned over $21 billion in 2018 from "personal information in U.S. digitial advertising," while Facebook earned over $11 billion, and several other platforms raised billions annually).

[114] *Global Requests for User Information*, *supra* note 5.

its requests for user information in 2012, it has received no more than eleven wiretap requests in any half of a calendar year, while it routinely receives thousands of search warrants during the same intervals, and such warrants have only grown more common over time.[115] Similar trends have emerged among other major tech companies: In the six months spanning Apple's latest transparency report (July to December 2021), the U.S. government issued Apple 4,052 device subpoenas and 3,033 account subpoenas, and zero wiretap orders.[116] Meta's January to June 2022 transparency report (including Facebook, Instagram, and other products) showed 104 orders pursuant to the Wiretap Act, but tens of thousands of requests for access to stored communications under the SCA.[117]

In short, warrants issued under the SCA lack the accountability mechanisms given to wiretaps and have increasingly become routine. Accordingly, such orders allow law enforcement to secretly search through our personal information with relative ease. The result is that consumers may never know when they are the target of these broad powers.

II. OUR ANCIENT, STRINGENT RULE OF ANNOUNCEMENT

This Part places delayed notice searches in their broader historical context. It explains how, at common law and until very recently, warrants executed without notice violated the Fourth Amendment's announcement rule. Section II.A discusses how from the Middle Ages in England to the early nineteenth century in the United States, the announcement rule had no exceptions. Section II.B discusses how exceptions to the rule have developed since 1822, and how over many decades the announcement rule ultimately became, by the 1990s, a component of the warrant requirement. The rationale for this transformation was rooted in three concerns that an announcement might (1) enable suspects to escape, (2) destroy evidence, or (3) violently retaliate against an officer. Section II.C explains how, in today's digital context, these concerns simply do not apply. It argues that because the justifications for exceptions to the announcement rule do not apply in a digital context, the announcement rule's traditional logic suggests for digital searches, announcement should be presumptively required.

A. *The Common Law Requirement of Notice*

Supreme Court Fourth Amendment doctrine in recent decades has departed from traditional, more stringent requirements that searches of houses and paper for incriminating evidence require notice to the owner of the places or things being searched. Yet the reasons that the Court has given for relaxing the ancient

[115] *Id.*

[116] APPLE TRANSPARENCY REPORT: GOVERNMENT AND PRIVATE PARTY REQUESTS JULY 1 - DECEMBER 31, 2021, at 14 (2023), https://www.apple.com/legal/transparency/pdf/requests-2021-H2-en.pdf [https://perma.cc/E9B3-8NS6].

[117] *Government Requests for User Data: United States*, *supra* note 6.

notice requirement for searches do not apply convincingly to cloud searches. To understand the significance of the Supreme Court's relatively recent shift in jurisprudence, it is helpful to understand the requirement's original construction. Accordingly, this Section describes the notice requirement in its original form, one which was used from the Middle Ages into the nineteenth century.

The legal principle that law enforcement officials must announce their presence before conducting a search long predates the U.S. Constitution. In fact, the concept served as a prerequisite for forcible entry into private property under English common law as early as the thirteenth century. When the 1275 Statute of Westminster codified English law, it formalized the Distress Act, "The Remedy if a Distress be impounded in a Castle or Fortress."[118] Under this law, should any person take the "beasts of [an]other" and "withhold them" in a "Castle or Fortress" and "the Beasts be solemnly demanded by the Sheriff, or by some other Bailiff of the King's," then "*after such time as the Lord or Taker shall be admonished to make Deliverance by the Sheriff or Bailiff* . . . the King . . . shall cause the said Castle or Fortress to be beaten down without Recovery."[119] In short, the King's agents could only break into a dwelling to retrieve the stolen animals after they had instructed the owner of the dwelling to deliver them.

The King's Bench opinion in the influential *Semayne's Case* reiterated this announcement rule and summarized its original rationales.[120] The court deemed the Distress Act "but an affirmance of the common law,"[121] and explained that

> In all cases when the King is . . . party, the sheriff (if the doors be not open) may break the party's house, either to arrest him, or to do other execution of the K.'s process, if otherwise he cannot enter. But before he breaks it, he ought to signify the cause of his coming, and to make request to open doors . . . for the law without a default in the owner abhors the destruction or breaking of any house (which is for the habitation and safety of man) by which great damage and inconvenience might ensue to the party, when no default is in him; for perhaps he did not know of the process, of which, if he had notice, it is to be presumed that he would obey it.[122]

In this passage, we can see both the traditional rule of announcement along with its original rationale: If officers do not announce their presence, the property owner might mistake them for intruders and respond with violence or refuse entry. In the latter case, officers would only be able to execute their duties by breaking into the house, which the court sought to deter. The court therefore held officers to be responsible for announcing themselves before entry to avoid confusion about how the owner was entitled to respond, thus minimizing the risk of injury and property damage. The rule also presumed the occupants' innocence

[118] Statute of Westminster 1275, 3 Edw. c. 17 (Eng.).

[119] *Id.*

[120] Semayne's Case (1604) 77 Eng. Rep. 194, 194.

[121] *Id.* at 196.

[122] *Id.* at 195-96.

and good faith—officers could not assume that occupants would disobey their commands after learning of their lawful authority.

Crucially, courts did not inquire into whether officers' failure to announce themselves would actually have led to violence or property damage. Nor did they inquire whether any given occupant would have obeyed an officer's command had the occupant known of the officer's authority. Both the principle of presumed innocence and the policy consideration of property preservation weighed against such case-by-case inquiries. To administer the announcement rule on a case-by-case basis would have effectively invalidated the rule.

Courts continued to follow *Semayne's Case* as precedent for generations afterward.[123] Significantly, in this premodern body of caselaw, the announcement rule had no recognized exceptions. In the 1802 case *Ratcliffe v. Burton*,[124] the English Court of Common Pleas held that:

> The law of England, which is founded on reason, never authorises such outrageous acts as the breaking open every door and lock in a man's house without any declaration of the authority under which it is done . . . No entry from the books of pleading has been cited in support of this justification, and *Semayne's case* is a direct authority against it.[125]

It is worth noting that none of the authorities discussed thus far made a connection between the rule of announcement and the warrant requirement. In these cases, even if a warrant was not technically required, the courts nonetheless insisted that the authorities provide notice of the search. In *Institutes of The Lawes of England*, the leading sixteenth and seventeenth century English jurist Sir Edward Coke discussed the common law requirements for officers forcing entry into a house.[126] According to Coke, officers typically needed both a felony warrant and an indictment for stolen goods to enter private property.[127] The principal exception to this rule[128] was for arrests pursuant to the "hue and cry,"[129] analogous to the modern doctrine of hot pursuit. Under this doctrine, when pursuing a felon "upon hue and cry of one that is slain or wounded. . . or robbed, the kings officer that pursueth may (*if denyall be made*) breake a house to apprehend [him]."[130] In other words, while hue and cry might have been an exception to the warrant requirement, it was not an exception to the

[123] *See supra* notes 16-17 and accompanying text.

[124] (1802) 127 Eng. Rep. 123 (CP).

[125] *Id.* at 126-27.

[126] COKE, *supra* note 16, at 176-77.

[127] *Id.*

[128] Coke wrote of other exceptions to the warrant requirement, such as arrests on suspicion or breach of the peace. COKE, 2 INSTITUTES OF THE LAWS OF ENGLAND 51-55 (1642) (W. Clarke & Sons eds., 1817). However, Coke does not exempt officers from their *notice* obligations in such circumstances, only from their obligation to obtain a warrant.

[129] COKE, *supra* note 16, at 176.

[130] *Id.* (emphasis added).

announcement rule. The announcement rule applied regardless of whether a warrant was required.

In short, three features defined the premodern announcement rule and distinguished it from its contemporary form: The premodern announcement rule (1) had no exceptions, (2) was unrelated to any warrant requirement, and (3) derived its rationale from the desire to prevent violence, preserve property, and presume innocence. The rule also shared a key commonality with its modern incarnation, in that announcement was required when entering any private building that individuals would typically occupy or use, and not just their residences.

These key features persisted in the American colonies, both in their statutes and applications of English common law. A Massachusetts Bay 1697 excise statute allowed officers to forcibly enter "houses, cellars and warehouses in which he shall be informed any . . . goods or merchandizes are concealed . . . *if the owner or possessor of such houses, cellars or warehouses shall deny entrance thereinto*."[131] Early Virginia law provided that "[A]ny sheriff or constable by warrant from such justice . . . shall have power and authority, and is hereby required to enter any suspected houses and to break open all doors in the day time (*the keys of such doors having been first demanded and refused to be delivered*)."[132] Similarly, Virginia law provided that although an officer may

> search suspected places or houses . . . he cannot break open doors barely to search, unless the person against whom the hue and cry is levied be there, and then it is true he may . . . but it must always be remembered, that in case of breaking open a door, there must be first notice given to them within of his business, and a demand of entrance, and refusal, before doors can be broken.[133]

Consistent with the notion of "common" law, in the colonies as in England, there were no exceptions to the announcement rule even in cases where officers did not need a warrant. For instance, an officer pursuing a fleeing felon could "break the doors of the house to take him, *if upon demand he will not yield himself to the constable*."[134] Similarly, under the controversial "writs of assistance"—general warrants for Crown officers which helped bring the colonies to the brink of rebellion—the law still required that Crown agents notify the occupants prior to entry.[135]

---

[131] An Act for Granting Unto His Majesty Several Duties of Impost, Excise, and Tunnage of Shipping, ch. 3 (1697), *in* 1 THE ACTS AND RESOLVES OF THE PROVINCE OF THE MASSACHUSETTS BAY 269, 271 (Boston, Wright & Potter 1869) (emphasis added).

[132] An Act for Reviving Several Publick Warehouses for the Inspection of Tobacco, ch. X (1778), *in* WILLIAM WALLER HENING, 9 THE STATUTES AT LARGE; BEING A COLLECTION OF ALL THE LAWS OF VIRGINIA 482, 507 (Richmond, George Cochran 1821) (emphasis added).

[133] *Id.* at 241.

[134] HALE, *supra* note 16, at 94 (emphasis added).

[135] An Act for Preventing Frauds and Regulating Abuses in His Majesties Customes 1662, 14 Car. II, c. 11, § IV (Eng.) ("And it shall be lawfull to or for any person or person authorized

Crucially, colonial laws required some form of notice even when no occupant was present to admit officials. When a sheriff was unable to serve process on an individual because the individual was absent from their home or place of business, Virginia law required the sheriff to leave "an attested copy of the writ" at the premises.[136] Likewise, Massachusetts adopted the English custom[137] requiring officials who removed goods from a searched property to leave behind a notice describing the items they had taken.[138] By the same token, nocturnal laws were heavily disfavored in most states and considered presumptively unreasonable.[139] These requirements arose from the principle "implied, by natural justice," that "in the construction of all laws . . . no one ought to suffer any prejudice thereby, without having first an opportunity of defending himself."[140] To withhold notice of a search or seizure was thus to deny occupants a fair defense.

Such examples show that by the time of the American Revolution and the ratification of the Constitution and Bill of Rights, there was overwhelming consensus that the announcement rule should be stringently applied. The legal historian William J. Cuddihy observes that "Every legal manual for American justices of the peace between 1788 and 1791 forbade unannounced, forcible entry to accomplish an arrest."[141] Two such manuals used wording nearly identical to *Semayne's Case*, stating "that no one can justify the breaking open of another's door to make an arrest, unless he first signify to those in the house the cause of his coming, and [request] them to give him admittance."[142] Most state statutes and legal manuals contained some equivalent provision.[143] It is from within this legal tradition that we should understand the origins of the Fourth Amendment in 1791, which was understood in part to forbid

by Writt of Assistance . . . in the day time to enter and go into any House Shop Cellar Warehouse or Room or other place and in case of resistance to breake open Doores . . . ."); *see* Note, *Announcement in Police Entries*, 80 YALE L.J. 139, 144-45, 145 n.26 (1970).

[136] HENING, *supra* note 132, at 409.

[137] *See, e.g.*, WILLIAM HAWKINS, 3 A TREATISE OF THE PLEAS OF THE CROWN 182 (1795); Wilkes v. Wood (1765), 98 ENG. REP. 489, 498-99 (KB); Entick v. Carrington (1765) 95 Eng. Rep. 807, 818 (KB).

[138] An Act in Addition to an Act, Entitled, "An Act in Addition to an Act, Entitled, "An Act for Preventing All Commerce and Illegal Correspondence with the Enemies of the United States of America.", ch. 32 (1782), *in* ACTS AND LAWS OF THE COMMONWEALTH OF MASSACHUSETTS 84, 86-87 (1890).

[139] WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602-1791, at 745 (2009).

[140] HENING, *supra* note 132, at 203.

[141] CUDDIHY, *supra* note 139, at 749.

[142] JAMES PARKER, CONDUCTOR GENERALIS 27 (1788); *see* JOHN FAUCHERAUD GRIMKÉ, THE SOUTH CAROLINA JUSTICE OF PEACE 18 (3d ed. 1810) (articulating virtually identical statement but for set of commas); CUDDIHY, *supra* note 139, at 749 (citing *Conductor Generalis*, *The South Carolina Justice*, and "similar book for North Carolinians" for all declaring same principle against "unannounced, forcible entry to accomplish an arrest").

[143] CUDDIHY, *supra* note 139, at 749-50.

"unreasonable processes" such as unannounced searches.[144] Crucially, however, the text of the Fourth Amendment explicitly applies these prohibitions not just to places of habitation, but to other property as well in the form of "papers" and "effects."[145]

The legal system of the newly independent "United States" in adopting and possibly strengthening these common law protections thus began with the same absolute announcement rule that had persisted since at least the thirteenth century in England. As the following Section will illustrate, courts would later carve broad categories of exceptions out of this default rule. However, such exceptions were designed to address practical problems that, as we will see, are not ones that digital searches tend to produce.

B. *The Notice Requirement in the Modern Era*

For much of the eighteenth and nineteenth centuries, most American courts followed the premodern announcement rule.[146] Gradually, however, courts began to recognize exceptions to the rule. One such instance was the 1822 Connecticut decision in *Read v. Case*,[147] in which the Supreme Court of Errors held that officers need not announce their presence where "[i]mminent danger to human life" existed.[148] Regarding the necessity of announcement, the majority explained that:

> Although this is the general rule, and established on principles of wise policy, there are cases not within the reason of it, and which, manifestly, form a just and reasonable exception. The one displayed on the record, is clearly of this description. The principal had resolved . . . to resist even to the shedding of blood. Under these circumstances, he was not within the reason and spirit of the rule requiring notice; nor was the bail obliged by law to make a demand, that would probably issue in the destruction of his life.[149]

It is important to recall in this context that prior rulings such as *Semayne's Case* considered it immaterial whether a given occupant might respond with violence—such case-by-case inquiries were previously thought to contradict the presumption of innocence.[150] Indeed, Judge John Thompson Peters made precisely this argument in dissent, arguing that the *Semayne's Case* standard

---

[144] *Id.* at 749.

[145] U.S. CONST. amend. IV.

[146] *See, e.g.*, Kelsy v. Wright, 1 Root 83, 84 (Conn. 1783); Oystead v. Shed, 13 Mass. (12 Tyng) 520, 523 (1816); Haggerty v. Wilber, 16 Johns. 287, 288-89 (N.Y. Sup. Ct. 1819); Burton v. Wilkinson, 18 Vt. 186, 189-190 (1846); Barnard v. Bartlett, 64 Mass. (10 Cush.) 501, 502-03 (1852); Commonwealth v. Reynolds, 120 Mass. 190, 196-97 (1876).

[147] 4 Conn. 166 (1822).

[148] *Id.* at 170.

[149] *Id.*

[150] *See supra* notes 120-22 and accompanying text.

should continue to apply.[151] Here, however, the majority introduced a new consideration: Occupants might respond with violence *because* the occupant knew that the intruder was a law enforcement officer.[152] The majority thus prioritized the safety of government officers over the presumption of innocence.

While some courts continued to maintain the strict premodern announcement rule,[153] other courts continued to find exceptions to the ancient rule. In 1854, the Kentucky Court of Appeals held in *Hawkins v. Commonwealth*[154] that officers need not announce their presence in criminal cases because "such disclosure of his purpose and demand of entrance would in many cases defeat the very object [of arrest], by giving the offender notice of his danger and an opportunity of effecting his escape."[155] Again, we see the shift from prioritizing occupants' rights to authorities' needs. Recall again that under the premodern rule, announcement was required even in "hue and cry" hot pursuit cases where an officer arrested a fleeing suspect whose crime the officer had witnessed.[156] Here, concern that a suspect might use announcement to evade officers again superseded the considerations of property damage, presumed innocence, and possible violence where the occupant mistook the officer for an intruder.

Among the first Supreme Court decisions to address notice was *Miller v. United States*.[157] *Miller* interpreted a 1948 statute codifying the announcement rule[158] rather than the Constitution itself, but in characteristic fashion under the processes of common law constitutionalism, the case would later influence the Supreme Court's jurisprudence on the Fourth Amendment's notice requirements.[159] In *Miller*, police who lacked a warrant failed to adequately identify themselves before effecting a narcotics arrest.[160] Because the government did not allege exigent circumstances like those in *Read* and similar decisions, the Court did not decide whether the statute permitted such exceptions to the announcement rule.[161] However, absent such exigent circumstances, the Court interpreted the statute as codifying the notice requirement in *Semayne's Case*, holding that "[t]he requirement stated in *Semayne's Case* still obtains. It is reflected in 18 U.S.C. § 3109 . . . . It applies . . . whether the arrest is to be

[151] *Read*, 4 Conn. at 171 (Peters, J., dissenting) (opposing majority's exception to announcement rule articulated in *Semayne's Case* on grounds that any threat to life did not rise to level of necessity in this case).

[152] *See id.* at 170.

[153] *See, e.g.*, Accarino v. United States, 179 F.2d 456, 465 (D.C. Cir. 1949) (invalidating arrest because arresting officers failed to announce presence before forced entry).

[154] 53 Ky. (14 B. Mon.) 318 (1854).

[155] *Hawkins*, 53 Ky. at 397.

[156] *See supra* notes 128-30 and accompanying text.

[157] 357 U.S. 301 (1958).

[158] Act of June 25, 1948, Pub. L. No. 772, ch. 645, § 3109, 62 Stat. 683, 820 (codified at 18 U.S.C. § 3109).

[159] *See infra* notes 174-75 and accompanying text.

[160] *Miller*, 357 U.S. at 302-04.

[161] *Id.* at 309.

made by virtue of a warrant, or when officers are authorized to make an arrest for a felony without a warrant."[162]

As would become a recurring theme in notice cases, the officers in *Miller* had neither adequately announced themselves nor obtained a warrant. The Court, as the above passage shows, treated the notice and warrant requirements as separate inquiries. This practice accorded of course with the premodern announcement rule. However, the Court would soon deviate from this practice and merge the two inquiries, which would become the modern announcement rule's most distinctive feature.

Thus, in the 1963 case *Wong Sun v. United States*,[163] the Supreme Court began assessing the notice and warrant requirements jointly. In that case, federal narcotics agents arrested a San Francisco man who claimed he had bought the narcotics he possessed from a Leavenworth Street laundromat owner whom he knew only as "Blackie Toy."[164] At 6:00 AM that morning, the officers found a Leavenworth Street laundromat owned by a man named James Wah Toy, but "nothing in the record . . . identifie[d] James Wah Toy and 'Blackie Toy' as the same person."[165] When one officer knocked on the door and asked about picking up a dry-cleaning order, James Wah Toy stated that he had not yet opened the shop for business and began to close the door.[166] The officer identified himself as a narcotics agent and revealed his badge, whereupon Toy slammed the door and retreated down the hall.[167] The agents then kicked down the door, pursued Toy into his adjacent apartment, and arrested him.[168] The officers found no narcotics in Toy's apartment.[169] Toy argued that his arrest was the product of unreasonable search and seizure, in violation of the Fourth Amendment.[170] The government argued that "Toy's flight down the hall when the supposed customer at the door revealed that he was a narcotics agent" yielded probable cause, regardless of whether such cause had existed previously.[171]

In finding for Toy, the Supreme Court reiterated its holding in *Miller*, recalling that it had then "held that when an officer insufficiently or unclearly identifies his office or his mission, the occupant's flight from the door must be regarded as ambiguous conduct."[172] The Court noted that because the officer had made "no effort . . . to ascertain whether the man at the door was the 'Blackie Toy'" identified by their informant, "Toy's refusal to admit the officers and his

[162] *Id.* at 308-09.
[163] 371 U.S. 471 (1963).
[164] *Id.* at 473.
[165] *Id.* at 474.
[166] *Id.*
[167] *Id.*
[168] *Id.*
[169] *Id.*
[170] *Id.* at 477.
[171] *Id.* at 482.
[172] *Id.*

flight down the hallway thus signified a guilty knowledge no more clearly than it did a natural desire to repel an apparently unauthorized intrusion."[173] The Court in essence held that failure to give proper announcement nullified the state's ability to infer probable cause from a suspect's flight or refusal of entry. Although the Court only held that the lack of proper announcement barred one specific method of showing probable cause, it was the Court's first suggestion that the notice requirement was linked to the standards of proof typically seen in warrant cases.

Mere months later in *Ker v. California*,[174] the Court ruled squarely on the requirements of Fourth Amendment notice.[175] In this case, officers who suspected George Ker of purchasing marijuana contacted Ker's landlord, who gave them a key to Ker's apartment. With no announcement or identification, the officers opened Ker's door, seized marijuana from his apartment, and arrested Ker and others.[176] California case law provided for "an exception to the notice requirement where exigent circumstances are present"[177] (similar to the scenario the Court had contemplated in *Miller*), but Ker argued that this exception violated the Fourth Amendment.[178] The Supreme Court affirmed Ker's conviction, but no group of justices formed a majority.[179] Justice Tom Clark and three others held that the Constitution permitted such an "exigent circumstances" exception, asserting that, in contrast to *Miller*,

> justification for the officers' failure to give notice is uniquely present. In addition to the officers' belief that Ker was in possession of narcotics, which could be quickly and easily destroyed, Ker's furtive conduct in eluding them shortly before the arrest was ground for the belief that he might well have been expecting the police.[180]

This passage contains the two key characteristics of modern notice jurisprudence previously discussed: (1) the "exigent circumstances" consideration historically used to justify exemptions from the warrant requirement, and (2) prioritizing officers' ability to safely make arrests over the presumption of innocence and avoidance of violence where occupants mistake police for unlawful intruders.

Writing for a group of four other justices, Justice William Brennan offered a more classical account of the announcement rule. According to Brennan, "even on the premise that there was probable cause by federal standards for the arrest of George Ker, the arrests of these petitioners were nevertheless illegal, because the unannounced intrusion of the arresting officers into their apartment violated

---

[173] *Id.* at 483.

[174] 374 U.S. 23 (1963).

[175] *See generally id.*

[176] *Id.* at 28-29.

[177] *See id.* at 39.

[178] *See id.* at 37-38.

[179] *See id.* at 24, 43-44, 46.

[180] *Id.* at 40.

the Fourth Amendment."[181] In so doing, his opinion adopted two of the key classical justifications for the premodern announcement rule—first, that the presumption of innocence demanded that the announcement rule be enforced,[182] and second, that the creation of new exceptions to the announcement rule would be the proverbial exceptions that would "devour the rule."[183] Importantly, Justice Brennan's analysis suggested that nothing about modern policing had eroded the need for announcement—his opinion strongly suggests that advances in occupants' abilities to evade arrest, retaliate violently against police, or destroy evidence did not alter the fundamental logic behind the rule, and that the presumption of innocence remained paramount in a modern context.

Because *Ker* offered merely a plurality opinion on the constitutional requirements of notice, some subsequent lower courts waived the notice requirement where there were exigent circumstances,[184] while others did not.[185] This division in authority persisted for over three decades until the Supreme Court granted certiorari in *Wilson v. Arkansas*.[186] Unlike in the 1963 cases, the officers in *Wilson* had obtained a warrant.[187] They then entered Wilson's house through an unlocked screen door and arrested Wilson, announcing themselves only as they were entering the house.[188] In a unanimous opinion, the Court formally reframed the announcement rule as merely a factor in determining the need for a warrant rather than a necessity in its own right, completing the jurisprudential shift first hinted at in *Wong Sun*.[189] The Court held that "the common-law principle of announcement" is "an element of the reasonableness inquiry under the Fourth Amendment."[190] Rather perplexingly, the Court then erroneously claimed that the announcement rule "was never stated as an inflexible rule requiring announcement under all circumstances. See *Ker* v. *California*, 374 U.S. 23, 38 (1963) (plurality opinion) ('[I]t has been recognized from the early common law that . . . breaking is permissible . . . under certain circumstances')."[191] This assertion suggested that the common law had

[181] *Id.* at 46 (Brennan, J., concurring in part and dissenting in part).

[182] *Id.* at 56.

[183] *Id.* at 61-62.

[184] *See, e.g.*, Hopkins v. State, 500 P.2d 579, 581 (Okla. Crim. App. 1972).

[185] *See, e.g.*, State v. Cook, 564 P.2d 877, 883 (Ariz. 1977).

[186] 514 U.S. 927 (1995).

[187] *Id.* at 929.

[188] *Id.* Note that under both the premodern and modern rules, if an occupant is present, officers can only satisfy the announcement rule by announcing themselves *before* entering a house, not during or after. *See id.* at 931-32, 934.

[189] *Id.* at 934.

[190] *Id.* Although the Court here refers to announcement as an "element" of the reasonableness inquiry (which might imply an indispensable requirement), the Court elsewhere deems announcement to be "among the factors to be considered in assessing the reasonableness of a search or seizure." *Id.* The Court's opinion clearly indicates the view that announcement can be dispensed with in certain circumstances.

[191] *Id.* (citing Ker v. California, 374 U.S. 23, 38 (1963) (plurality opinion)).

historically allowed officers to break into houses *without announcement* in certain circumstances, despite the lengthy historical record to the contrary recounted earlier.[192] As we have seen, breaking into houses historically had been permissible in certain conditions, but doing so *unannounced* had not.[193]

Wilson's reasoning left many contemporary scholars unsatisfied,[194] and in 1997 the Court revised its approach in *Richards v. Wisconsin*,[195] outlining the basic framework of the announcement rule as it stands today.[196] In *Richards*, the Court unanimously held that "In order to justify a 'no-knock' entry, the police must have a reasonable suspicion that knocking and announcing their presence, under the particular circumstances, would be dangerous or futile, or that it would inhibit the effective investigation of the crime by, for example, allowing the destruction of evidence."[197]

Two important features of the modern announcement rule emerged in *Richards*. First, as indicated above, the Court required officers to have reasonable suspicion, rather than probable cause, that one of the above scenarios applied. The Court considered this "the appropriate balance between the legitimate law enforcement concerns at issue in the execution of search warrants and the individual privacy interests affected by no-knock entries."[198] Second, the Court required a "case-by-case evaluation of the manner in which a search was executed."[199] The Court noted that creating categories of exceptions, as some post-*Wilson* lower courts had done, would undermine the rule's very purpose, observing that:

> [a]rmed bank robbers, for example, are, by definition, likely to have weapons, and the fruits of their crime may be destroyed without too much difficulty. If a *per se* exception were allowed for each category of criminal investigation that included a considerable—albeit hypothetical—risk of danger to officers or destruction of evidence, the knock-and-announce element of the Fourth Amendment's reasonableness requirement would be meaningless.[200]

---

[192] *See supra* Section II.A.

[193] *Id.*

[194] *See, e.g.*, WAYNE R. LAFAVE, SEARCH & SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.8(a) (5th ed. 2019); Robert J. Driscoll, *Unannounced Police Entries and Destruction of Evidence After* Wilson v. Arkansas, 29 COLUM. J.L. & SOC. PROBS. 1, 25-28 (1995); Mark Josephson, *Fourth Amendment—Must Police Knock and Announce Themselves Before Kicking in the Door of a House?*, 86 J. CRIM. L. & CRIMINOLOGY 1229, 1261-62 (1996); Matthew A. Kern & Kyle A. Scott, *We Hear You Knocking, But You Can't Come In: The Supreme Court's Application of Common Law in Cases of Knock and Announce Entry*, 7 CONN. PUB. INT. L.J. 55, 68 (2008).

[195] 520 U.S. 385 (1997).

[196] *See id.* at 394.

[197] *Id.*

[198] *Id.*

[199] *Id.* at 392.

[200] *Id.* at 394.

Analysis of this sort suggests a Court finessing the announcement rule to arrive at what it perceived as a reasonable policy outcome. The term "appropriate balance" in the Court's justification for its new standard indicated this trend. Moreover, the Court's logic in barring categories of exceptions to the announcement rule could easily justify barring exceptions altogether, as Justice Brennan had argued in *Ker*.[201] The Court, however, did not go this far, presumably viewing such a rule as inappropriately discounting the "legitimate law enforcement concerns" it referenced.[202] Although the Supreme Court has since issued several other important notice rulings,[203] the standard from *Richards* generally remains in force today.[204]

C. *The Announcement Rule and § 2703*

To restate the foregoing, the modern history of the announcement rule has been marked by at least three key deviations from its original form. First, the rule has begun to balance the need to prevent violence from mistaken identity, preserve property, and presume innocence against officers' ability to safely and effectively conduct searches, seizures, and arrests.[205] Second, the rule shifted from a hard rule to one that could be dispensed with on a case-by-case basis in certain exigent circumstances.[206] Third, the announcement rule is no longer a distinct requirement but has been folded into the overall warrant inquiry.[207] However, none of the rationales for these three shifts are applicable to § 2703 warrants for digital evidence.

All three of the above shifts in notice jurisprudence predate ECPA measurably. The current balance-of-interests formulation and exigent circumstances exceptions can be fairly traced back in one form or another to the 1820s, while the integration of the notice and warrant requirements began in the 1960s.[208] Yet § 2703 searches are in many key respects more analogous to searches conducted in the premodern era of notice. In the physical world, there are many ways occupants can frustrate police searches of a private building: they may resist with violence, attempt to destroy or conceal evidence, or escape. As

[201] *See* Ker v. California, 374 U.S. 23, 57 (1963) (Brennan, J., dissenting).

[202] *See Richards*, 520 U.S. at 394.

[203] *See, e.g.*, Kentucky v. King, 563 U.S. 452, 462-63 (2011) (holding "warrantless entry to prevent the destruction of evidence is reasonable and thus allowed" even in police-created exigent circumstances); United States v. Banks, 540 U.S. 31, 40 (2003) (holding Fourth Amendment permitted officers breaking down door of house in narcotics raid following fifteen to twenty seconds of silence after officers knocked).

[204] *See, e.g.*, Missouri v. McNeely, 569 U.S. 141, 142 (2013) (rejecting government's request for "a *per se* rule . . . that exigent circumstances necessarily exist when an officer has probable cause to believe a person has been driving under the influence of alcohol because [blood alcohol content] evidence is inherently evanescent").

[205] *See supra* Section II.A.

[206] *See supra* Section II.B.

[207] *See supra* Section II.B.

[208] *See supra* Section II.B.

our society has urbanized and technology has advanced, judicial concern for such possibilities has increased. But these concerns are inapplicable when we are talking about searching stored communications. Digital communications stored on a corporations' cloud server have no "occupant" who could violently resist officers, destroy evidence, or evade capture based solely on announcement. In these respects, searches pursuant to § 2703 warrants more closely resemble searches conducted in times when frustrating such searches was far less practically feasible. Because the impetus for each aforementioned shift was a potential undesirable reaction by an occupant, there is a strong argument that the Supreme Court's modern notice jurisprudence simply should not extend to searches of places or entities that cannot be occupied. We suggest that in the absence of some other, new and significant rationale for a departure from the strict premodern announcement rule, such searches follow that rule's requirement that notice is constitutionally necessary.

The principle that the premodern rule should apply where no occupant is present is not merely one that is suggested by longstanding constitutional tradition; it is also compatible with modern announcement jurisprudence. The practice of granting exceptions to the announcement rule in exigent circumstances would require no modification at all. Recall that the holdings in early cases like *Read* and *Hawkins* were formulated as exceptions to the premodern announcement rule rather than as a redefinition of the rule itself (in contrast to later cases like *Wilson* and *Richards*).[209] Although their exceptions encompassed a wide array of cases and severely limited the rule, they quite clearly did not extend to cases where there was no threat of violence against an officer and no suspect whose escape an announcement might enable.[210] One does not need to be an ardent originalist to see that the ancient principle is here fully consistent with the context of searches in our digital present.

Similar reasoning applies to the Court's balancing of occupants' rights and officers' ability to safely effectuate arrests seen in *Wilson*, *Richards*, and Justice Clark's *Ker* opinion. In *Richards*, for instance, the Court lowered the evidentiary standard for when police could decline to announce themselves in order to strike "the appropriate balance between the legitimate law enforcement concerns at issue in the execution of search warrants and the individual privacy interests affected by no-knock entries."[211] Yet none of the legitimate interests the Court mentions in its opinion apply when searching stored communications, as each of these interests presupposes an occupant on the premises.[212] The same is true for the officers' interests which the above *Wilson* and *Ker* opinions were designed to protect.

Reasoning of this sort is also fully consistent with recent Fourth Amendment cases involving slightly different digital contexts. When the Court has balanced

[209] *See supra* Section II.B.

[210] *See supra* Section II.B.

[211] Richards v. Wisconsin, 520 U.S. 385, 394 (1997).

[212] *See generally id.* (explaining flaw in analogy between physical and digital entry).

suspects' rights against officers' ability to safely effectuate arrests in other contexts, it has adopted the principle that digital evidence cannot pose a threat to officers, and has allowed the suspects and defendants to assert their Fourth Amendment rights successfully. In *Riley*, the Court held that "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape,"[213] and therefore did little to counterbalance the (augmented) privacy interests arrestees had in their digitally stored information. In *Riley*, this reasoning was used to foreclose an exception to the warrant requirement in digital contexts,[214] but it should equally foreclose exceptions to the notice requirement in such contexts. In a striking similarity to *Richards*, *Riley* "assess[ed], on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[215] This balancing test is nearly identical to the one in *Richards* described above, and yields the same conclusion when applied.

Even the reasoning behind reframing the announcement rule as merely one factor in the warrant requirement test presupposes an occupant. The Court in *Wilson* formally instituted this practice to reflect the announcement rule's "flexible" status (although this flexibility originated far later than the Court implied).[216] However, the rule had only ever been made "flexible" where courts had deemed the needs of officers to require it.[217] While it does no harm to reframe notice as an *indispensable element* of the reasonableness inquiry, it should not be considered merely one factor in assessing reasonableness in such cases, because officers conducting such searches do not encounter the circumstances contemplated in *Wilson* and *Richards*. Accordingly, virtually all the shifts in jurisprudence regarding Fourth Amendment notice requirements presuppose an occupant, and it therefore need not apply where occupants' possible responses are not at issue.

To be clear as a methodological matter, our argument is compatible with an originalist reading of the Fourth Amendment but does not depend on it. The *Wilson* and *Richards* holdings clearly deviate from the announcement rule's understood scope when the Fourth Amendment was adopted. Even the idea of exigent circumstances exceptions to the announcement rule is a significant departure from the original inflexible rule. However, our argument for a baseline requirement of notice in digital search cases does not require overturning *Wilson* or *Richards*, nor would it invalidate all exigent circumstances exceptions to the announcement rule. It merely requires accepting the proposition that searches in the cloud contain none of the justifications for exceptions to the announcement rule that are present in searches of physical property, and that courts should

[213] Riley v. California, 573 U.S. 373, 387 (2014).

[214] *See infra* Part III.

[215] *Riley*, 573 U.S. at 374 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[216] *See supra* Section II.B.

[217] *See supra* Section II.B.

therefore distinguish unannounced cloud searches from cases like *Wilson* and *Richards.*

To be sure, there are differences between unannounced cloud searches today and physical searches under the premodern announcement rule. A digital search does not destroy physical property, as breaking into a house often does. And there may well be other differences as well. However, cloud searches often uncover information whose value lies in its secrecy—a list of passwords, the locations of valuable objects, notes and records, or ideas the owner may not wish to share publicly. Therefore, the potential to damage property interests still exists in some sense. Of course, there is also the possibility of damage to privacy interests that had laid at the center of the Fourth Amendment since *Katz*. Moreover, the premodern announcement rule contained no exception where property interests could not be damaged—creating such an exception would have contradicted the presumption of innocence. Because there is no "occupant" or anyone analogous in a SCA search, and no basis for extending the announcement rule to situations where no occupant is present, courts should never retroactively allow law enforcement to withhold notice in such circumstances. Part III will demonstrate that, under this recommendation, the provisions of § 2703 authorizing warrants to be executed without notice are unconstitutional.

III. THE UNCONSTITUTIONALITY OF UNANNOUNCED § 2703 SEARCHES

This Part shifts the frame of analysis from legislative and constitutional history to doctrine. It argues that without satisfying the announcement rule, the provisions of § 2703 allowing the government to withhold notice if it has obtained a warrant are unconstitutional. It begins by reviewing the modern requirements for executing a constitutionally protected search, namely that law enforcement officers must obtain and lawfully execute a warrant or find an applicable exception to the warrant requirement. It then reviews *Warshak*'s holding that SCA search orders are constitutionally protected searches, and *Riley*'s indication that law enforcement authorities cannot use exceptions to the warrant requirement based on suspects' ability to escape, destroy evidence, or threaten officers to obtain digitally stored evidence warrantlessly. It then discusses *Carpenter*'s tacit affirmation of the above holdings, and its indication that *Riley* applies specifically to the SCA. It establishes that delayed notice orders are unconstitutional under the proposed return to the inflexible announcement rule described in Part II.

A Fourth Amendment "search" is considered to occur "when an expectation of privacy that society is prepared to consider reasonable is infringed."[218] This standard consists of two inquiries: "[F]irst, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second,

[218] United States v. Jacobsen, 466 U.S. 109, 113 (1984); *accord* California v. Ciraolo, 476 U.S. 207, 211 (1986); Smith v. Maryland, 442 U.S. 735, 740 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

is society willing to recognize that expectation as reasonable?"[219] Thus, if an individual has exhibited a subjective expectation of privacy that society recognizes as objectively reasonable, a search has occurred. Searches "conducted without warrants" are "*per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[220]

Law enforcement officials seeking to justify accessing an individual's "houses, papers, or effects" must therefore satisfy at least one of the following three inquiries: (1) Was notice given prior to entry? (2) If not, was a warrant lawfully executed without notice? (3) If not, was there an exception to the warrant requirement? If the answer to each of these three questions is "no," the search violates the Fourth Amendment. Searches conducted without notice under § 2703 by definition do not satisfy the first inquiry. Part II of this Article demonstrated that exigent circumstances cannot satisfy the second. This Section will show that compelled disclosure of communications under the SCA is a search within the Fourth Amendment's meaning, that no applicable exception allows law enforcement to dispense with the warrant requirement, and that such orders should therefore be considered unconstitutional.

Several court decisions have placed restraints on SCA searches since ECPA's passage. Perhaps the first case relevant to § 2703's constitutional implications was the 2010 Sixth Circuit case, *United States v. Warshak*.[221] The case arose when Steven Warshak was convicted of several crimes involving his business, including money laundering and fraud,[222] based in part on evidence the government collected by seizing over 27,000 of Warshak's emails.[223] The government obtained the emails via a subpoena in January 2005 and a court order in May 2005, but "Warshak did not receive notice of either the subpoena or the order until May 2006."[224] Warshak argued that he had a reasonable expectation of privacy in his emails, and that this seizure violated his Fourth Amendment rights.[225] Although the Sixth Circuit declined to overturn Warshak's conviction because it found the government to have "relied in good faith on provisions of the Stored Communications Act,"[226] it nevertheless issued two key holdings regarding the scope of permissible conduct by law enforcement under the SCA.

First, the Sixth Circuit held that Warshak "enjoyed [a] reasonable expectation of privacy in his emails," and therefore "government agents violated his Fourth

[219] *Ciraolo*, 476 U.S. at 211 (citing *Smith*, 442 U.S. at 740).

[220] *Katz*, 389 U.S. at 357.

[221] 631 F.3d 266 (6th Cir. 2010) (holding that plaintiff enjoyed reasonable expectations of privacy in emails through internet service provider and government violated Fourth Amendment by encouraging provider to give them plaintiff's emails).

[222] *See id.* at 276-82.

[223] *See id.* at 283.

[224] *Id.*

[225] *See id.* at 281-82.

[226] *Id.* at 274.

Amendment rights" by compelling his internet service provider to produce the emails without a warrant.[227] The Court noted that the case's facts satisfied the modern standard[228] for Fourth Amendment protection.[229] It found that "Warshak had a subjective expectation of privacy in the contents of his emails"[230] as "his 'entire business and personal life was contained within the . . . emails seized,'"[231] and that this expectation was an objectively reasonable one.[232] The court observed that "Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[233] It further noted that in recent years, "email has become 'so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification,'"[234] and therefore "requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve."[235] Note the reasoning that emails merit Fourth Amendment protection because of their "fundamental similarities" to "traditional forms of communication."[236] Intuitively, this reasoning would equally apply to most communications covered by the SCA—the Act largely governs "traditional forms of communication" adapted to modern storage methods, such as a written document stored on a server rather than on paper.[237] Although *Warshak* was not a Fourth Amendment challenge to any provision of § 2703, it implied that such a challenge was possible.

In *Warshak*, the Sixth Circuit issued another holding with even greater bearing on the constitutionality of § 2703 searches conducted without notice. It held that "[t]he government may not compel a commercial ISP [Internet Service Provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause," and "[m]oreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[238] Emails searched under the SCA, in essence, were subject to the Constitution's warrant requirement, not merely the warrant requirements in the SCA. As discussed above, the same should apply

[227] *Id.* at 266.

[228] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 211 (1986); Smith v. Maryland, 442 U.S. 735, 740 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[229] *Warshak*, 631 F.3d at 284.

[230] *Id.*

[231] *Id.* (alteration in original) (quoting Brief for Appellant, *Warshak*, 631 F.3d at 284).

[232] *See id.* at 284-88.

[233] *Id.* at 285-86.

[234] *Id.* at 286 (alteration in original) (quoting City of Ontario v. Quon, 560 U.S. 746, 760 (2010)).

[235] *Id.*

[236] *Id.* at 285.

[237] *Id.*

[238] *Id.* at 288.

to most or all communications within the SCA's scope. This is notable because, since *Wilson*, notice has been a prerequisite for obtaining a warrant, absent exigent circumstances.[239] However, § 2703 does not require officials to announce searches of (1) communications stored remotely,[240] or (2) electronic communications stored for over 180 days.[241] Therefore, if the constitutional notice requirement is inflexible when searching stored communications, such unannounced searches violate the Fourth Amendment.

Four years after *Warshak*, the Supreme Court significantly restricted officers' ability to dispense with the warrant requirement when conducting digital searches in *Riley*.[242] Ever since the 1969 case *Chimel v. California*,[243] the Court had allowed officers conducting lawful arrests to warrantlessly "search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape" or "to prevent . . . concealment or destruction" of evidence.[244] In essence, the possibility that a suspect might respond to a lawful arrest with violence, attempt to escape, or try to destroy or conceal evidence entitled officers to search arrestees (and their immediate surroundings)[245] without a warrant, regardless of whether any concern about such threats actually existed. This exception to the warrant requirement became known as the "search incident to arrest" rule ("SITA").[246] *Riley*, however, excluded digital information on arrestees' cell phones from SITA, and held that "[t]he police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[247]

The Court in *Riley* reasoned that "[a]bsent more precise guidance from the founding era . . . whether to exempt a given type of search from the warrant requirement" should be decided "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[248] Using this test, the Court concluded that while SITA "strikes the appropriate

[239] *See* Wilson v. Arkansas, 514 U.S. 927, 934 (1995); Richards v. Wisconsin, 520 U.S. 385, 394 (1997) (clarifying when exceptions to announcement rule exist).

[240] 18 U.S.C. § 2703(b)(1)(A).

[241] *Id.* § 2703(a).

[242] Riley v. California, 573 U.S. 373, 403 (2014).

[243] 395 U.S. 752, 767-68 (1969).

[244] *Id.* at 763; *see also* Arizona v. Gant, 556 U.S. 332, 343 (2009) (holding that *Chimel*'s rule allowed officers to search vehicle when passenger compartment was within unsecured arrestee's reach, or when officers reasonably suspected that evidence of crime of arrest was present in vehicle); United States v. Robinson, 414 U.S. 218, 235-36 (1973) (holding that *Chimel* applied to all custodial arrests, regardless of whether any specific concern about loss of evidence or threats against officers existed).

[245] *See Chimel*, 395 U.S. at 763.

[246] *See, e.g.*, *id.* at 762; *Gant*, 556 U.S. at 335; *Robinson*, 414 U.S. at 227.

[247] *Riley*, 573 U.S. at 373.

[248] *Id.* at 385 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

balance in the context of physical objects,"[249] searching digital information on cell phones posed a far greater privacy intrusion while doing far less to promote legitimate government interests. It noted that searches of digital data posed "no comparable risks" reminiscent of "the two risks identified in *Chimel*—harm to officers and destruction of evidence,"[250] as "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[251] On the other hand, the Court observed that such searches "place vast quantities of personal information literally in the hands of individuals," in contrast to the far smaller privacy intrusion resulting from the "brief physical search" contemplated in past SITA cases.[252]

Riley did not concern an SCA search, but the balancing test and analysis from *Riley* apply equally well to the SCA. Like searches of digital information on cell phones, a stored communication "cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape."[253] However, access to accounts containing stored communications, such as email and online file storage accounts, reveal the same "vast quantities of personal information" which the Court deemed an unreasonable privacy intrusion in *Riley*.[254] While *Warshak* held that the warrant requirement applied to the SCA, *Riley*'s reasoning, if applied to SCA searches, eliminated the primary means of obtaining an exception to this requirement.

In 2018, the Supreme Court further reinforced the *Warshak* and *Riley* holdings in *Carpenter v. United States*.[255] In *Carpenter*, "after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were granted court orders to obtain the suspects' cell phone records under the Stored Communications Act."[256] Under these SCA orders,

> Wireless carriers produced CSLI [cell site location information] for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated the Fourth Amendment.[257]

[249] *Id.* at 386.
[250] *Id.*
[251] *Id.* at 387.
[252] *Id.* at 386.
[253] *Id.* at 387.
[254] *Id.* at 386.
[255] 138 S. Ct. 2206, 2217-18 (2018).
[256] *Id.* at 2208-09.
[257] *Id.* at 2209.

The Supreme Court granted Carpenter's motion, holding that "[t]he Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search" and therefore required a warrant.[258]

Although *Carpenter* dealt with a specific category of records rather than the constitutionality of any provision of the SCA, its holding contained two important points about the SCA in general: First, it rejected Justice Alito's dissenting argument that "the warrant requirement simply does not apply when the Government acquires records using compulsory process."[259] Instead, it observed that "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy."[260] In essence, *Carpenter* treated CSLI as *Warshak* treated emails, effectively adopting *Warshak*'s holding that "[t]he government may not compel a commercial ISP to turn over the contents . . . without first obtaining a warrant based on probable cause."[261] Indeed, the Court strongly suggested that anytime "the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party,"[262] the warrant requirement should apply, calling such a principle "sensible."[263] This expanded reading of *Warshak* would strongly imply that the warrant requirement applied to all types of communications covered by the SCA.

Second, the Court indicated that the above analysis from *Riley* applied to the SCA. The Court approvingly cited *Riley* both for its balancing test[264] and its differentiation of physical and digital searches.[265] Indeed, three dissenting justices understood the majority opinion to "establish a balancing test" where "[f]or each 'qualitatively different category' of information . . . the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party," although they disagreed with such a framework.[266] The majority did not affirmatively state that its reasoning in *Riley* applied to all communications stored remotely or electronically, but it clearly found the reasoning described above applicable to SCA cases.

To recap, four principles emerge from *Warshak*, *Wilson*, *Riley*, and *Carpenter*. First, per *Warshak*, the Fourth Amendment requires a warrant for SCA searches of communications with "fundamental similarities" to "traditional forms of communication."[267] Second, per *Riley*, the only exceptions to the

[258] *Id.*

[259] *Id.* at 2221.

[260] *Id.*

[261] United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[262] *Carpenter*, 138 S. Ct. at 2222 (first quoting *id.* at 2230 (Kennedy, J., dissenting); and then citing *Warshak*, 631 F.3d at 283-88)).

[263] *Id.*

[264] *Id.* at 2214.

[265] *Id.* at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."); *see Riley*, 573 U.S. at 386.

[266] *Id.* at 2231.

[267] *Warshak*, 631 F.3d at 285-86.

warrant requirement that might relate to such searches—those based on "harm to officers and destruction of evidence"—do not apply to digitally stored information.[268] Third, per *Carpenter*, *Warshak*'s central holding is tacitly affirmed[269] and *Riley* applies to SCA cases.[270] Fourth, because SCA searches must comply with the requirements for executing a warrant, officials must either provide notice before conducting the search or show that the notice requirement can be waived, per *Wilson*.[271]Accordingly, § 2703 searches where notice is withheld are unconstitutional unless the notice requirement is waivable.[272] Because, as shown in Part II above, the notice requirement should never be waived where no occupant can exist, such searches violate the Fourth Amendment.[273] Part IV will discuss how to best rectify this problem.

IV. THE NEED FOR WIRETAP-ACT-LIKE SAFEGUARDS FOR UNANNOUNCED CLOUD SEARCHES

This Part offers solutions to the problem we have outlined thus far. We believe that because litigation is likely to continue to prove incapable of resolving ECPA's Fourth Amendment problems in the context of secret and delayed-notice searches, the best solution to these problems would be for Congress to repeal all sections of the SCA authorizing delayed notification, specifically § 2703(b)(1)(A) and the provision of § 2703(a) governing communications stored electronically for over 180 days. Section IV.A outlines the logistical challenges that litigants wishing to challenge § 2703 warrants issued without notice will face. Section IV.B sets out a fairer set of notice requirements for a future version of ECPA that would comply with the demands of the Fourth Amendment. It argues that Congress's goal should be to provide subjects of such searches with the same presumption of innocence and property rights as the original notice requirement, including the adjoining Fourth Amendment right to be secure in one's papers and effects. It also argues that these goals can only be achieved by implementing safeguards like those ECPA requires for wiretaps, which contain much more stringent restrictions on law enforcement's collection, use, and disclosure of information than traditional warrants.

A. *Practical Obstacles to Litigation*

Although there are ample grounds to challenge § 2703 warrants executed without notice under the Fourth Amendment, litigating such cases poses enormous practical difficulties.[274] Even if future litigation invalidates preclusion-of-notice orders and cloud service providers routinely notify

[268] Riley v. California, 573 U.S. 373, 386 (2014).

[269] *See Carpenter*, 138 S. Ct. at 2222.

[270] *See supra* notes 264-69 and accompanying text.

[271] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).

[272] *See id.*

[273] *See supra* Part II.

[274] *See supra* Part III.

customers of all SCA orders concerning their data, many challenges remain. Because the warrants in question prevent targets from learning of their existence before they are executed, it is difficult to challenge such warrants unless the government brings criminal charges based on the evidence they yield.[275] However, targets of SCA orders are unlikely to ever be criminally charged.[276] As former U.S. Magistrate Judge Stephen William Smith notes,

> There are no good data on the number of persons targeted by these orders but never charged with a crime. However, the government's response to a recent FOIA request suggests the number is quite large. In *ACLU v. U.S. Dep't of Justice*, 655 F.3d 1 (D.C. Cir. 2011), the government was asked to provide docket information for any case in which an individual was prosecuted after the government obtained an order for cell phone location data without a showing of probable cause. In response, the DOJ produced a list of only 255 criminal prosecutions over a period of approximately seven years after September 11, 2001. . . . Given that thousands of such orders were issued by magistrate judges during this period, and that the first judicial decisions requiring probable cause for cell site information were not issued until 2005, it is reasonable to infer that far more law-abiding citizens than criminals have been tracked in this fashion.[277]

Moreover, logistical difficulties would persist even if one of the rare targets charged with a crime were to challenge an SCA warrant's constitutionality. To begin with, defendants may not be able to suppress evidence against them even if they demonstrate a Fourth Amendment violation.[278] As Smith observes, "Even if a constitutional violation is shown, relief may be denied if the officer acted in good faith."[279] Likewise, ECPA does not provide a "statutory suppression remedy" and instead authorizes "a post-execution civil action against the provider, [where] good faith reliance on a court order is an absolute defense."[280]

Even if a defendant did pursue such a motion despite the poor prospects of upside, it would be unlikely to set a precedent broad enough to invalidate the relevant SCA provisions.[281] As Smith observes, only a few ECPA cases have ever reached federal appeals courts.[282] Moreover, even if a motion to suppress evidence from an SCA order does reach the appellate courts, judges may decide the case without adjudicating the constitutionality of any part of § 2703.[283] *Warshak* and *Carpenter* illustrates this dynamic. According to Smith, by the time *Warshak* reached the Sixth Circuit, "magistrate judges were issuing tens of

---

[275] *See* Smith, *supra* note 7, at 327.

[276] *Id.* at 328 n.83.

[277] *Id.* (citation omitted).

[278] *See id.* at 327.

[279] *Id.* at 327 n.81 (citing United States v. Leon, 468 U.S. 897 (1984)).

[280] *Id.* (citing 18 U.S.C. §§ 2510-22, 2707(e)).

[281] *Id.* at 326.

[282] *Id.*

[283] *Id.* at 326-27.

thousands of [cell phone tracking] orders every year without appellate guidance."[284] Rather than hold any particular provision of the SCA unconstitutional, the Sixth Circuit then held that the government's *application* of the SCA violated the Fourth Amendment, ruling that "to the extent that the SCA purports to permit the government to obtain [the contents of a subscriber's] emails warrantlessly, the SCA is unconstitutional."[285] In short, many thousands of SCA orders were issued before a single federal appeals court invalidated a single application of SCA orders.[286] Getting such cases to the Supreme Court is an even more daunting task, and, as *Carpenter* demonstrates, the Court may invalidate an SCA order without invalidating the provision authorizing it.[287] In the meantime, untold numbers of law-abiding citizens will have their personal information searched without notice or recourse.[288]

Because of these logistical challenges, it will likely fall to Congress to amend the SCA provisions concerning delayed notice orders. Specifically, Congress should amend the SCA by repealing § 2703(b)(1)(A) (allowing warrants for communications stored remotely to be searched without notice), adding warrants to the list of orders that cannot be executed without notifying subscribers/customers in § 2703(b)(1)(B), and amending § 2703(a) to give communications that have been stored electronically for over 180 days the same protections against unannounced searches as those stored for up to 180 days and to require authorities to notify customers in all cases.[289] The following Section will argue that the constitutional notice requirement can only be satisfied by imposing a stricter "necessity" standard for withholding notice, analogous to ECPA's regulation of wiretapping.

B. *Towards Appropriate Notice for Cloud Communications Searches*

The goal of any revision to the standards for withholding notice should be to protect the principles underlying the original notice requirement: presuming innocence and preserving property rights (including the adjoining right to privacy in one's papers and effects guaranteed by the Fourth Amendment). Likewise, the requirements should not be waivable merely because law enforcement has obtained a valid warrant or shown an exception to the warrant requirement. For such a standard, Congress can look to the Wiretap Act's requirements.[290] As noted above, the Wiretap Act requires law enforcement officials to show special need and Department of Justice or high-level state approval before wiretapping a phone.[291] Additionally, agents must minimize the

[284] *Id.* at 326.
[285] United States v. Warshak, 631 F.3d 266, 289 (6th Cir. 2010).
[286] *See* Smith, *supra* note 7, at 326-27.
[287] *Id.* at 326.
[288] *See id.* at 326-28.
[289] *See supra* Part I.
[290] 18 U.S.C. §§ 2510-22.
[291] *Id.* § 2518(7).

interception of communications and justify each use and disclosure of information they intercepted,[292] and must provide "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous" to the authorizing judge.[293]

The principles underlying the original notice requirement demand this level of stringency at a minimum. The standard on investigative procedures is equivalent to the constitutional necessity standard.[294] As Professor Jonathan Witmer-Rich explains, the *exigent circumstances* standard "justif[ies] a warrantless search even if police could have conducted the same search—and found the same evidence—with a warrant."[295] By contrast, under a *necessity* standard, the proposed method of investigation must be "the only reasonable way to obtain the evidence sought."[296] As applied to unannounced § 2703 searches, this standard would require law enforcement to provide a full and complete statement of the consequences they could reasonably expect from failure to provide notice, along with supporting evidence.[297] In other words, law enforcement should have to rebut the presumption of innocence *before* conducting an unannounced search.[298] In a digital context, courts should not be able to retroactively waive the notice requirement.

Additionally, preserving the Fourth Amendment's guarantee of security in one's papers and effects requires use and disclosure minimization rules resembling those of the Wiretap Act.[299] Congress should require law enforcement to minimize as much as possible the amount of information searched without notice. It should also require that each use and disclosure of the information collected "is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure," as the Wiretap Act requires.[300] This process parallels the colonial laws requiring officers who sought to search houses to leave behind an attested copy of writs when no occupant was available to admit them.[301] If individuals do not know which of their communications have been searched and for what purpose, they are forced to conduct themselves as though all their communications have been

[292] *Id.* §§ 2517, 2518(5); *see also* SEC v. Rajaratnam, 622 F.3d 159, 175 (2d Cir. 2010) (holding that U.S. Attorney's Office "may not be authorized to provide these materials [collected from wiretaps] to [another] civil enforcement agency").

[293] 18 U.S.C. § 2518(1)(c).

[294] Witmer-Rich, *supra* note 12, at 163-64.

[295] *Id.* at 142 (citing Kentucky v. King, 563 U.S. 452 (2011)).

[296] *Id.* at 164.

[297] *Id.* at 147 n.107.

[298] *See supra* Section II.A.

[299] U.S. CONST. amend. IV.

[300] 18 U.S.C. § 2517(1) (2006).

[301] *See, e.g.*, HENING, *supra* note 132, at 409.

searched.[302] As discussed above, this prospect comes with enormously detrimental consequences for free expression.[303]

Authorities have not offered compelling justification for a more lenient standard. A 2004 DOJ White Paper supporting the PATRIOT Act's[304] similar authorization of covert surveillance[305] focused on accommodating "both the urgent need to conduct a search and the equally pressing need to keep the ongoing investigation confidential."[306] Many of its examples involved intercepting drugs or other physical evidence from criminal organizations without revealing that the government was conducting an investigation.[307] While this consideration is certainly legitimate, it does not clearly apply to the cloud, where copies of evidence can be brought into custody without removing the original file or message from its location. Moreover, because both providers and customers can access information stored in the cloud, evidence of a communication can be preserved even if a customer deletes the communication from their account.[308] Where law enforcement must monitor potential criminal conspiracies but need not seize tangible evidence, it may request authorization under the Wiretap Act and comply with the Act's added restrictions on use, disclosure, and minimization.[309] It is not immediately apparent what investigative capabilities law enforcement would lose if held to the same standard for searches of stored communications.

CONCLUSION

The notice requirement has been a crucial bulwark protecting the presumption of innocence and property rights since the thirteenth century. The requirement is equally essential to maintaining freedom of expression, as it assures citizens that law enforcement authorities are not regularly scrutinizing their papers and effects unannounced. These principles are crucial to the Fourth Amendment. However, the privileges § 2703 confers on law enforcement do not conform to these principles. While the Supreme Court currently takes a more flexible posture toward notice, its rationales for departing from the traditional, baseline rule do not apply to searches in the cloud where there is no occupant to physically endanger officers, escape, or destroy evidence. Without notice, a § 2703 warrant therefore cannot be properly executed. Moreover, as the *Riley*

[302] *See supra* Section II.A.

[303] *See supra* Part III.

[304] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of 18 U.S.C.).

[305] 18 U.S.C. § 3103a.

[306] U.S. DEP'T OF JUST., DELAYED NOTICE SEARCH WARRANTS: A VITAL AND TIME-HONORED TOOL FOR FIGHTING CRIME 1 (2004), http://www.justice.gov/sites/default/files/dag/legacy/2008/10/17/patriotact213report.pdf [https://perma.cc/TKA7-HGQD].

[307] *Id.* at 4-7.

[308] *See supra* note 4 and accompanying text.

[309] *See supra* Section I.A.

and *Carpenter* decisions indicate, unannounced § 2703 warrant searches are subject to Fourth Amendment protection, and no exception to the warrant requirement exists. Such warrants therefore violate the Fourth Amendment.

Given the enormous practical obstacles to litigation, we believe that Congress should repeal the provisions in § 2703(a) and § 2703(b)(1)(B) allowing unannounced searches, and replace them with laws requiring the stricter necessity standard to perform an unannounced search. The burden should fall on law enforcement to rebut the presumption of innocence and show that they are preserving occupants' rights to the greatest possible extent before searching stored communications unannounced. Doing so would not place an unreasonable burden on law enforcement's ability to do its job in a way that is consistent with the fundamental rights we all enjoy. It would merely close an accidental loophole that changes in technology have blown open, and bring federal electronic surveillance law for stored communications back into alignment with the long-held protective regime for wiretaps.

Today, ECPA governs much of our everyday communication.[310] If law enforcement can regularly disregard the Constitution's notice requirement when performing searches under ECPA, our Fourth Amendment protections become severely curtailed. The future of Americans' digital civil liberties mandates certainty that authorities do not regularly monitor them without their knowledge. Without such certainty, we must all constantly ask ourselves whether the government might retaliate against us based on our private communications. Currently, we lack such certainty, and only Congress can secure our assurance in our constitutional protections. Our ancient, hard-won, and fragile civil liberties may well depend on it doing so.

[310] *See* Griffith, *supra* note 1.