2018

A Cognitive Theory of the Third-Party Doctrine and Digital Papers

H. Brian Holland
Texas A&M University School of Law, hbholland@law.tamu.edu

A COGNITIVE THEORY OF THE THIRD-PARTY DOCTRINE AND DIGITAL PAPERS

H. Brian Holland[*]

ABSTRACT

For nearly 200 years, an individual's personal papers enjoyed near-absolute protection from government search and seizure. That is no longer the case. With the widespread adoption of cloud-based information processing and storage services, the third-party doctrine operates to effectively strip our digital papers of meaningful Fourth Amendment protections.

This Article presents a new approach to reconciling current third-party doctrine with the technological realities of modern personal information processing. Our most sensitive data is now processed and stored on cloud-computing systems owned and operated by third parties. Although we may consider these services to be private and generally secure, the law does not currently require the government to obtain a warrant to access our stored information. The third-party doctrine creates a sweeping exception to the warrant requirement for any information exposed to a third party—even where that third party is an automated computing system rather than a human. As a result, our personal papers now receive no more protection than any other piece of potential evidence. In practical terms, they receive less. This ahistorical approach undermines the essential balance between an individual's interest in privacy and the public's interest in law enforcement. Many have identified and tried to rectify the privacy problems created by the shift to third-party cloud-computing systems, but it has proven difficult to articulate a limitation to the third-party doctrine that is both consistent with existing principles and feasible in practice.

This Article begins with the intimate connection among freedom of thought, privacy of thought, and the longstanding enumeration of "papers" as a distinct object of Fourth Amendment protection. This historical understanding of the relationship between human thought and private papers, which prior generations recognized intuitively, now finds strong support in contemporary cognitive science. Modern models of human cognition reveal how papers serve as cognitive artifacts performing cognitive tasks. These models furnish a set of proxy characteristics for reliably singling out those personal papers whose protection would most likely serve constitutional values. The result is a coherent and workable method for bringing needed discipline to the third-party doctrine and restoring equilibrium to information privacy.

---

* Professor of Law, Texas A&M University School of Law. Sincere thanks to Malinda L. Seymore, Saurabh Vishnubhakat, and Kymberlie Welp, and to the participants in the Internet Law Works-in-Progress conference, Intellectual Property Works-in-Progress conference, and University of Oklahoma College of Law faculty exchange program for the many helpful comments.

TABLE OF CONTENTS

INTRODUCTION

For almost two centuries, an individual's personal papers enjoyed near-absolute constitutional protection from governmental search and seizure, even against an otherwise valid warrant.[1] In the latter half of the twentieth century, however, these constitutional bulwarks quickly fell away,[2] leaving personal papers "no more likely to be excluded from evidence than [almost] any other item."[3] For several decades, the Fourth Amendment's warrant requirement nevertheless worked as a fairly effective safeguard of personal papers.[4] Although

1. *See* Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 568 (2016) [hereinafter Donohue, *Digital World*] ("For nearly two hundred years, the government could *not* obtain private papers—even with a warrant—when they were to be used as evidence of criminal activity."); *see also* Boyd v. United States, 116 U.S. 616, 633 (1886) (describing the broad protection for personal papers provided by both the Fourth and Fifth Amendments).

2. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 472 (1976) (finding no violation of the Fifth Amendment right against compulsory self-incrimination where the target of a search warrant was not required to prepare, produce, or authenticate personal papers); Warden v. Hayden, 387 U.S. 294, 309–310 (1967) (eliminating the Fourth Amendment mere evidence rule as a basis for heightened protection for personal papers).

3. Craig M. Bradley, *Constitutional Protection for Private Papers*, 16 HARV. C.R.-C.L. L. REV. 461, 473 (1981); *see* Donald A. Dripps, *"Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure*, 103 J. CRIM. L. & CRIMINOLOGY 49, 50–51 (2013) (describing the shift from "extraordinary exemption" to mere effects); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 597–98 (2017) (noting that personal papers are much less protected by the Fourth Amendment in modern times than they once were).

4. The "warrant requirement" refers to the following standard: "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, this Court has said that reasonableness generally requires the obtaining of a judicial warrant." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (citing Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989)). A warrant may only be issued upon a showing of probable cause to believe that contraband or

no longer afforded exceptional protection, under most circumstances personal papers maintained a sort of derivative protection as material objects physically located within well-established "constitutionally protected area[s]."[5]

The notion of real property as a constitutionally protected area had essentially survived the transition from the property-and-trespass approach of *Olmstead v. United States*[6] to the expectation-of-privacy test adopted following *Katz v. United States*.[7] Likewise, the Court consistently recognized an individual's reasonable expectation of privacy as to certain containers located within those physical spaces, such as office furniture[8] and desktop computers,[9] where personal papers were likely to be stored. Even those personal papers sealed in an envelope and entrusted to the post office for conveyance, and thus outside the direct control of the sender, could not be searched without a valid warrant, "as is required when papers are subjected to search in one's own household."[10] Thus, in an analog world of tangible documents—filed away in cabinets and computers, stored in homes and offices, and conveyed through first-class mail—most personal papers remained, as a practical matter, secure behind at least two layers of constitutional protection.

It was not long, however, before this relative stability was undermined by a radical transformation of the information environment, marked by the emergence of ubiquitous networked computing, digital data, electronic communications, and the commodification of information.[11] A vast array of common activities that were previously undertaken offline are now completed

---

evidence of a crime will be found. *Id.*

5. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting United States v. Jones, 565 U.S. 400, 406 n.3 (2012)) (noting the Supreme Court's long-standing jurisprudence linking a Fourth Amendment "search" to physical intrusion "on a constitutionally protected area").

6. 277 U.S. 438, 466 (1928) (holding that the wiretapping of conversations is not a search within the meaning of the Fourth Amendment, which requires actual physical examination of one's person, papers, tangible material effects, or home), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

7. 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (defining a Fourth Amendment search by reference to an intrusion into an individual's "constitutionally protected reasonable expectation of privacy").

8. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (citing various cases) (finding that even public employees have, in certain circumstances, "a reasonable expectation of privacy at least in [their] desk[s] and file cabinets").

9. *See, e.g.*, Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, 1240 (2012) (describing the traditional search of a computer as involving two entries, "one into the home or office, the other into the computer"); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 549 (2005) ("[T]he starting point for applying the Fourth Amendment to a computer hard drive is clear and generally uncontroversial: the Fourth Amendment applies to computer storage devices just as it does to any other private property.").

10. *Ex parte* Jackson, 96 U.S. 727, 733 (1878).

11. *See* OFFICE OF TECH. ASSESSMENT, OTA-CIT-293, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 3, 10 (1985), http://ota.fas.org/reports/8509.pdf [perma.cc/4KU2-P2EL] ("The existing statutory framework and judicial interpretations thereof do not adequately cover new and emerging electronic surveillance technologies.").

online, as we use the internet for communication, transactions, storage, and more.[12] These online activities generate enormous amounts of associated data,[13] as "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[14] Much of that data is processed and stored by third-party intermediaries and online service providers in the regular course of business.[15] Conveyance to and retention of a user's data by the third-party provider is no longer a byproduct of the commercial transaction between user and provider, but is rather at the operational core of the service infrastructure.[16] Intermediaries collect and use data "in order to route communications, detect spam and viruses, block computer hackers, or generate advertising revenue."[17] Online service providers retain "[e]-mails, web-surfing histories, cloud computing documents, search terms, and credit-card information."[18] It is an infrastructure designed not to conceal and control information but to expose that data as routine practice.

Given the vast quantity and expansive character of the data now held by third-party providers, the absence of appropriate statutory and constitutional protections threatens to undermine societal expectations for information privacy. Indeed, there is an emerging consensus that rapidly evolving computer and information technologies are outpacing the ability of our legal system to adapt to the realities of digital data, networked infrastructure, changing human behavior, and user expectations.[19] And with each advancement, that lag is compounded at an exponential rate.

How then should the law be revised to return equilibrium to information privacy? Prior proposals have generally proceeded along one of two routes: legislation modifying the Stored Communications Act[20] or reform of the Fourth Amendment's third-party doctrine. In regard to the latter, proposals to modify the doctrine can be difficult to formulate in part because its underlying rationale

---

12. *See* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 986 (2016); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) [hereinafter Tokson, *Automation*].

13. Tokson, *Automation*, *supra* note 12, at 588.

14. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

15. *See id.*

16. *See* Ahmed Shawish & Maria Salama, *Cloud Computing: Paradigms and Technologies*, *in* INTER-COOPERATIVE COLLECTIVE INTELLIGENCE: TECHNIQUES AND APPLICATIONS 39, 48–52 (Fatos Xhafa & Nik Bessis eds.) (Studies in Computational Intelligence Vol. 495, 2014) (describing the various models of third-party cloud services and the centrality of user data in each).

17. Tokson, *Automation*, *supra* note 12, at 602.

18. *Id.* at 588 ("These trillions of bytes of information can often be linked to the IP address and then the name and home address of the individual user.").

19. *See, e.g.*, Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 19–28 (2013) [hereinafter Bedi, *Facebook*] (reviewing various criticisms of the Fourth Amendment and third-party doctrine); Christina Raquel, *Blue Skies Ahead: Clearing the Air for Information Privacy in the Cloud*, 55 SANTA CLARA L. REV. 467, 468 (2015) (describing the Stored Communications Act as "[o]utdated and disjointed nearly three decades later").

20. 18 U.S.C. §§ 2701–2712 (2018) (providing a statutory framework for the disclosure of "stored wire and electronic communications and transactional records" held by third-party internet service providers).

remains unclear.[21] At various times, courts have described the exposure of information to a third party as negating an individual's expectation of privacy, as signifying voluntary consent to disclosure of that information by the third party, as assuming the risk that the information will simply find its way to government officials in one way or another, or as some combination of these theories.[22] Most reform proposals attack the validity of one or more of these justifications, often in the context of technological change.[23] Critics have argued, for instance, that the rule no longer reflects society's expectations, or that disclosing data online is no longer voluntary,[24] or that application of the third-party doctrine to certain forms of communication violates constitutional protections for interpersonal relationships.[25] Others have argued that user interactions with automated systems, where human observation is possible but unlikely, should not trigger the rule at all.[26] This represents only a partial accounting of the numerous proposals, which vary not only in concept but also in ambition. Some critics seek to eliminate the rule in its entirety, while others call only for modifications that might more equitably balance individual privacy interests against the interests of society and law enforcement.[27] It has proven difficult, however, to articulate both an animating rationale and limiting principles that fit comfortably within existing privacy doctrine and are workable in practice.[28]

---

21. *See, e.g.*, Bedi, *Facebook*, *supra* note 19, at 11–14 (discussing various theories asserted to justify the third-party doctrine); Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) [hereinafter Kerr, *Third-Party Doctrine*] (same).

22. *See* United States v. Graham, 824 F.3d 421, 427 (4th Cir. 2016) (discussing the various theories); *see also* Smith v. Maryland, 442 U.S. 735, 744 (1979) (assumption of risk); United States v. Miller, 425 U.S. 435, 442–43 (1976) (voluntariness and assumption of risk).

23. *See, e.g.*, Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith*, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, 7 (2016) (arguing that "in an IP-based communications environment, the concept of voluntary conveyance . . . is, at best, a legal fiction"); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 984–86 (2007) (arguing that individuals may retain a reasonable expectation of privacy in information shared with a third party); Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 482, 511–16 (2012) (presenting survey data purporting to "refute the assumption of risk rationale"); Sonia K. McNeil, *Privacy and the Modern Grid*, 25 HARV. J.L. & TECH. 199 (2011) (challenging the notion of the third-party doctrine as a doctrine of consent).

24. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (suggesting that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" in the digital age (first citing *Smith*, 442 U.S. at 742; then citing *Miller*, 425 U.S. at 443)).

25. *See generally* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011) (arguing that the current "aggressive form of third party doctrine" applied to online activities and communications does not reflect society's expectations of privacy); Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) (describing how the concept of knowing and voluntary disclosure is undermined by many technologies that society considers essential to daily living and that integrate the disclosure of information to third parties).

26. *See generally* Tokson, *Automation*, *supra* note 12 (arguing that the "courts' conflation of disclosure to automated systems with disclosure to human beings threatens online privacy").

27. *See, e.g.*, Bedi, *Facebook*, *supra* note 19, at 17–18 (reviewing various proposed remedies).

28. *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine*

This Article takes a different path. Accepting Justice Scalia's implicit invitation in *United States v. Jones*[29] to revisit the core enumerated objects of Fourth Amendment protection[30]—"persons, houses, papers, and effects"[31]—I explore the functional import of "papers" in the maintenance of personal privacy. For most of U.S. history, the significance of papers as a constitutionally protected area remained practically obscured by other, more expansive privacy doctrines like papers as property, shielded by the "mere evidence" rule;[32] papers as conveyed confidential messages entrusted to the U.S. mail;[33] and papers as effects, secured within private premises or closed containers.[34] Even as personal papers moved from the analog form to digitized files, the privacy analysis proceeded by analogy along these same lines: emails to letters, computers to file cabinets, and so on.[35] But as information technologies continue to evolve, placing "digital papers" beyond these traditional boundaries of what is private and what is public, we must consider Fourth Amendment protections for papers qua papers, apart from this protective overlay.

In this Article, I argue that the enumeration of papers as a discrete area of Fourth Amendment protection—distinct from trespass upon real and personal property (i.e., houses and effects) and bodily integrity (i.e., persons)—reflects a unique and substantial concern for the historical sanctity of "an individual's most private thoughts."[36]

---

of the Fourth Amendment, 13 FLA. COASTAL L. REV. 33, 42 n.47 (2011) (providing an extensive overview of various and diverse approaches to reforming the third-party doctrine).

29. 565 U.S. 400 (2012).

30. *See Jones*, 565 U.S. at 406–07 (holding that *Katz* supplemented, rather than replaced, traditional concerns about government trespass upon the four enumerated objects of Fourth Amendment protection).

31. U.S. CONST. amend. IV.

32. *See* Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1308–14 (2016) [hereinafter Donohue, *Original Fourth Amendment*] (discussing the history of the "mere evidence" rule). The "mere evidence rule" refers to the "former doctrine that a search warrant allows seizure of the instrumentalities of the crime (such as a murder weapon) or the fruits of the crime (such as stolen goods), but does not permit the seizure of items that have evidentiary value only (such as incriminating documents)." *Mere-Evidence Rule*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see also* Warden v. Hayden, 387 U.S. 294, 300 (1967) (explaining and rejecting the rule).

33. *See* Donohue, *Original Fourth Amendment*, *supra* note 32, at 1307 n.728 (quoting THOMAS M. COOLEY & VICTOR H. LANE, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 432 n.2 (7th ed. 1903)).

34. *See* Donohue, *Digital World*, *supra* note 1, at 678–79.

35. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting) (recognizing "letters held by mail carrier" and "e-mails held by Internet service provider" as limitations on the third-party doctrine (first citing *Ex parte* Jackson, 96 U.S. 727, 733 (1878); then citing United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010))); *Warshak*, 631 F.3d at 285–88 (6th Cir. 2010) (discussing the analogy of email to letters and phone calls); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (calling the "surveillance of e-mail addresses . . . conceptually indistinguishable from" that of physical mail); Trulock v. Freeh, 275 F.3d 391, 410 (4th Cir. 2001) ("Courts have not hesitated to apply established Fourth Amendment principles to computers and computer files, often drawing analogies between computers and physical storage units such as file cabinets and closed containers." (citing various cases)).

36. Eric Schnapper, *Unreasonable Searches and Seizures of Papers*, 71 VA. L. REV. 869, 890

Freedom of thought has been "recognized for centuries as perhaps the most vital of our liberties"[37] and "the central liberty in our constitutional system."[38] In the words of Justice Cardozo, "freedom of thought . . . is the matrix, the indispensable condition, of nearly every other form of freedom."[39] But although "[t]he freedom of individuals to control their own thoughts has been repeatedly acknowledged by the Supreme Court,"[40] the precise foundations and substance of that freedom remain somewhat uncertain.[41]

Freedom of thought has been primarily connected to First Amendment protections for speech, association, assembly, and the exercise of one's religious beliefs.[42] In this regard, the more inward freedom of thought holds only instrumental value (i.e., "value as a means to some other valuable end"),[43] with freedom of thought valued "as a way of promoting" these outwardly expressive liberties.[44] In addition, the "Court has also recognized the intersection of freedom of the mind, protected by the First Amendment, with the right to privacy."[45] As one scholar observed, "[t]he 'right of privacy' is more than a physical dwelling, . . . it is the 'privacy of thought.'"[46] Indeed, it has been argued that the "right of privacy [is] derive[d] from this respect for the individual mind in both its intellectual and its lurid workings."[47]

As the Constitution's central privacy provision, the Fourth Amendment reflects this relationship, preserving a protected sphere of respite and seclusion

---

(1985); *see also* Dripps, *supra* note 3, at 67–68 (describing concerns expressed in the early English cases that the seizure of personal papers exposed a man's secret thoughts).

37. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 388–89 (2008) [hereinafter Richards, *Intellectual Privacy*].

38. Marc Jonathan Blitz, *Freedom of Thought for the Extended Mind: Cognitive Enhancement and the Constitution*, 2010 WIS. L. REV. 1049, 1049 [hereinafter Blitz, *Freedom of Thought*].

39. Palko v. Connecticut, 302 U.S. 319, 326–27 (1937), *overruled by* Benton v. Maryland, 395 U.S. 784 (1969).

40. Doe v. City of Lafayette, 377 F.3d 757, 776 (7th Cir. 2004).

41. *See, e.g.*, Blitz, *Freedom of Thought*, *supra* note 38, at 1051 ("[A]s central as freedom of thought is to our constitutional system, it is also something of a mystery: the Supreme Court has never said exactly what this freedom is."); Adam J. Kolber, *Two Views of First Amendment Thought Privacy*, 18 U. PA. J. CONST. L. 1381, 1383 (2016) ("Many free speech cases trumpet our freedom of thought but say frustratingly little about the contours of the protection.").

42. *See* Marc Jonathan Blitz, *The Where and Why of Intellectual Privacy*, 87 TEX. L. REV. SEE ALSO 15, 15 (2009) [hereinafter Blitz, *Intellectual Privacy*] ("Freedom of thought has long been a celebrated part of First Amendment jurisprudence."). *But see* Kolber, *supra* note 41, at 1385 ("Constitutional protection of thought may emerge not only from the First Amendment, but also from the Fourth, Fifth, Eighth, and Fourteenth Amendments.").

43. Kenneth Einar Himma, *Privacy Versus Security: Why Privacy Is Not an Absolute Value or Right*, 44 SAN DIEGO L. REV. 857, 879 (2007) (comparing instrumental value to intrinsic value).

44. *See* Kolber, *supra* note 41, at 1386–87.

45. *City of Lafayette*, 377 F.3d at 777.

46. Claudia Tuchman, *Does Privacy Have Four Walls? Salvaging* Stanley v. Georgia, 94 COLUM. L. REV. 2267, 2280 (1994) (omission in original) (quoting Brief for Joel Hirschhorn, Esq., et al., on behalf of The First Amendment Lawyers' Ass'n, as Amici Curiae in Support of Appellant at 20, United States v. 12 200-Ft. Reels of Super 8mm. Film, 413 U.S. 123 (1973) (No. 70-2), 1972 WL 136206).

47. *Id.* at 2282.

as the "sanctuary where private reflections and inspirations may be created or recorded without fear."[48] As Justice Brandeis famously wrote in *Olmstead*:

> The makers of our Constitution . . . recognized the significance of man's spiritual nature, of his feelings and of his intellect . . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.[49]

Thus, just as freedom of thought holds instrumental value as a means of promoting outwardly expressive liberties, privacy of thought holds instrumental value as a means of promoting freedom of thought by preserving a protected sphere for the workings of the mind.

The history of the Fourth Amendment reflects this conspicuous connection, not only between freedom of thought and the right to privacy but to the enumeration of papers as a distinct area of protection. English cases and parliamentary debates of the late eighteenth century condemned the use of general warrants to search a man's papers, not simply because papers are a form of property but because papers reveal "the private workings of a person's mind."[50] In the United States, early state constitutions reflected this view as well, distinguishing textually (as does the Fourth Amendment) between papers and other forms of property.[51] And the Supreme Court, in one of its earliest privacy decisions, embraced the influence of English law on the structure and interpretation of the Fourth Amendment by, inter alia, acknowledging and adopting a special concern for invasions upon personal papers.[52] But these eighteenth-century decisions proved to be the "high-water mark" for the special status of papers.[53] Over the past century, broad rules based on binary distinctions (e.g., seclusion versus trespass, private versus public, and concealment versus disclosure) have subsumed this unique concern for personal papers almost to the point of vanishing.[54] The unique connection between personal papers and

---

48. Comment, *The Rights of Criminal Defendants and the Subpoena Duces Tecum: The Aftermath of* Fisher v. United States, 95 HARV. L. REV. 683, 699 (1982).

49. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

50. Dripps, *supra* note 3, at 66–67.

51. *See* Donohue, *Original Fourth Amendment*, *supra* note 32, at 1264–80 (discussing the various state provisions).

52. *See* Boyd v. United States, 116 U.S. 616, 623 (1886) ("The search for and seizure of stolen or forfeited goods, or goods liable to duties and concealed to avoid the payment thereof, are totally different things from a search for and seizure of a man's private books and papers for the purpose of obtaining information therein contained, or of using them as evidence against him.").

53. *See* Ferguson, *supra* note 3, at 597.

54. *See* Colleen Maher Ernst, Note, *Looking Back To Look Forward: Reexamining the Application of the Third-Party Doctrine to Conveyed Papers*, 37 HARV. J.L. & PUB. POL'Y 329, 334–42 (2014) (discussing the foundation of applying the third-party doctrine to private papers).

freedom of thought has been all but lost in the muddle of shifting Fourth Amendment theory and jurisprudence.

The goal of this Article is to offer a rationale for restoring the special status of papers by reestablishing their connection to and necessity for freedom of thought. More specifically, I argue that the significance of papers as a constitutionally protected area under the Fourth Amendment is in the function of papers and their digital equivalents as *cognitive artifacts*—objects or devices so broadly "incorporated into the very mechanisms of . . . human thought" as to demand privacy protection as a necessary condition to freedom of thought.[55] As part of a functionally integrated cognitive system, cognitive artifacts "represent, store, retrieve and manipulate information."[56] In practice, cognitive artifacts and technologies are quite familiar—from language and writing to computing and the internet.[57] And most of us can appreciate that these devices alter our thought processes by mediating our experiences and allowing us to offload various cognitive tasks. Although more modern technologies may illuminate our growing reliance on papers and their digital equivalents as cognitive artifacts, our reliance on cognitive artifacts is hardly a new phenomenon. For centuries, we have stored our personal memories in diaries, relied on books for facts about the larger world, and facilitated our relationships through handwritten letters.[58] The idea of papers as cognitive artifacts—as essential components of human cognitive processes—is entirely consistent with the experience of those who drafted and ratified the U.S. Constitution.

If we acknowledge our constitutional commitment to freedom of thought, then we must likewise recognize the need to safeguard the cognitive mechanisms that are necessary to effectuate that freedom. Those who gave birth to the Fourth Amendment understood this and expressly provided for such protections by securing "papers" against unreasonable search and seizure.[59] In the present information environment, however, where cognitive artifacts are no longer concealed within physical space but are instead distributed across third-party cloud-computing networks, existing jurisprudence fails this obligation.[60] This Article offers a proposal for restoring exceptional Fourth Amendment protections to papers and their digital equivalents by reforming current doctrine to meet the challenges of modern technologies.

---

55. Harry Collins, Andy Clark & Jeff Shrager, *Keeping the Collectivity in Mind?*, 7 PHENOMENOLOGY & COGNITIVE SCI. 353, 361 (2008) (Clark's "The Blind Carpenter: A Reply to Harry Collins").

56. Philip Brey, *The Epistemology and Ontology of Human-Computer Interaction*, 15 MINDS & MACHINES 383, 385 (2005) [hereinafter Brey, *Human-Computer Interaction*].

57. *See* Edwin Hutchins, *Cognitive Artifacts* [hereinafter Hutchins, *Cognitive Artifacts*] (discussing various examples of cognitive artifacts), *in* THE MIT ENCYCLOPEDIA OF THE COGNITIVE SCIENCES 126, 126–27 (R.A. Wilson & F.C. Kell eds., 2001).

58. *See generally* Donald A. Norman, *Cognitive Artifacts*, *in* DESIGNING INTERACTION: PSYCHOLOGY AT THE HUMAN-COMPUTER INTERFACE 17 (1991).

59. U.S. CONST. amend. IV.

60. *See* David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2218 (2009).

The Article proceeds in three sections. In Section I, I outline the relevant legal landscape, tracing the evolution of modern Fourth Amendment jurisprudence and the emergence of the third-party doctrine. In Section II, I describe the profound transformation of the digital age, focusing on digitized electronic communication and cloud computing. I then explore application of the third-party doctrine in an online environment where personal information is exposed to third-party intermediaries and online service providers as a matter of course. I conclude that, in practical application, the third-party doctrine creates an exception to the warrant requirement that all but swallows the general rule that warrantless searches are presumptively unreasonable.

In Section III, I propose exempting a relatively narrow class of digital papers from the third-party doctrine, thereby requiring the government to secure a Fourth Amendment warrant prior to a search or seizure of those documents from a third-party intermediary or online service provider. My proposal is constructed in three steps. In step one, I describe the relationship between freedom of thought as a constitutional commitment and privacy of thought as an essential condition for its realization. I then argue that freedom of thought and privacy of thought were historically connected to the enumeration of papers as a distinct object of Fourth Amendment protection. In step two, I seek to revive this connection by offering a new perspective on the role of personal papers in the processes of thought. I begin by introducing various models of human cognition and then explain how personal papers may be conceptualized as cognitive artifacts functioning as components of these systems. This account is consistent, I argue, with the intuition of prior generations that personal papers are deserving of extraordinary protection. In step three, I propose changes to the third-party doctrine intended to reestablish enhanced constitutional safeguards for certain personal papers. Integrating historical insight with modern cognitive theory, I set forth a method by which to identify a subset of personal papers, the protection of which is most likely to serve our commitment to freedom of thought.

I. THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE

The Supreme Court's Fourth Amendment jurisprudence has been described as "an incoherent mess."[61] The third-party doctrine has been called "the Fourth Amendment rule scholars love to hate."[62] But how did we reach this wretched state?

61. Nicholas Kahn-Fogel, *An Examination of the Coherence of Fourth Amendment Jurisprudence*, 26 CORNELL J.L. & PUB. POL'Y 275, 276, 278–92 (2016) (providing an extensive review of scholarship making this general argument).

62. Kerr, *Third-Party Doctrine*, *supra* note 21, at 563; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) ("[C]ountless scholars . . . have come to conclude that the 'third-party doctrine is not only wrong, but horribly wrong.'" (quoting Kerr, *Third-Party Doctrine*, *supra* note 21, at 564 (footnotes omitted))).

A. Fourth Amendment Jurisprudence

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause."[63] The Supreme Court has traditionally read the Amendment's substantive reasonableness clause and procedural warrant clause as interrelated, such that warrantless searches are said to be presumptively or even per se unreasonable.[64] In practice, however, the warrant requirement often offers little resistance.[65] Indeed, far from settling the question, the absence of a warrant merely reframes the inquiry. First, the lack of a warrant may be overcome by a showing that no search or seizure took place and therefore no warrant was required.[66] Second, even where a search has occurred, the government's actions may be excused under one of the numerous exceptions to the warrant requirement developed by the Court.[67] Finally, any surviving violation of the Fourth Amendment may be neutralized by failing to apply the exclusionary rule.[68]

It is this first question—whether a search has taken place—that dominates much of the Court's Fourth Amendment jurisprudence. Prior to 1967, a Fourth Amendment search was defined as a "physical intrusion [into] a constitutionally protected area in order to obtain information."[69] In applying this standard, a protected area was defined by an individual's property ownership or possessory rights in the object or location of the search.[70] And a physical intrusion was defined by reference to common law trespass.[71] The Court formally abandoned

---

63. U.S. CONST. amend. IV.

64. *See* Wayne D. Holly, *The Fourth Amendment Hangs in the Balance: Resurrecting the Warrant Requirement Through Strict Scrutiny*, 13 N.Y.L. SCH. J. HUM. RTS. 531, 541–43 (1997) (discussing the relationship between Fourth Amendment warrants and reasonableness, and the Supreme Court's asserted preference for the traditional warrant requirement); *see also Carpenter*, 138 S. Ct. at 2221 ("[W]arrantless searches are typically unreasonable . . . [unless they] fall[] within a specific exception to the warrant requirement." (citation omitted)).

65. Brent E. Newton, *The Real-World Fourth Amendment*, 43 HASTINGS CONST. L.Q. 759, 766 (2016) ("[I]n the vast majority of situations, a search warrant or an arrest warrant is *not* required for a 'reasonable' search or seizure to occur.").

66. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 31 (2001) ("[T]he antecedent question whether or not a Fourth Amendment 'search' has occurred is not so simple under our precedent.").

67. *See* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.1(b) (5th ed. 2017). There are six major exceptions to the warrant requirement (i.e., circumstances under which the government is permitted to conduct a search without first obtaining a warrant). *Id.* These exceptions include search incident to lawful arrest, the plain view exception, consent, stop and frisk, the automobile exception, and emergencies or hot pursuit. *Id.*

68. *See generally* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 1.1 (5th ed. 2017). The exclusionary rule provides that evidence obtained in violation of an individual's constitutional rights be excluded from evidence at trial. *Id.*

69. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring) (citing Silverman v. United States, 365 U.S. 505, 509–512 (1961)).

70. *See* United States v. Jones, 565 U.S. 400, 405 (2012) (discussing the Fourth Amendment's "close connection to property").

71. *See id.* at 405 ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass,

this property-and-trespass approach in *Katz*.[72] Observing that "the Fourth Amendment protects people, not places,"[73] the Court rejected formal, property-based limitations on the scope of Fourth Amendment protections,[74] focusing instead on whether government agents had violated the individual's "reasonable expectation of privacy."[75] Under this formulation, a Fourth Amendment search requires "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as [objectively] 'reasonable.'"[76] The *Katz* standard has governed Fourth Amendment jurisprudence for nearly five decades and remains the dominant standard for determining whether a search has taken place.[77]

In application, however, Fourth Amendment jurisprudence has been unable to shed the binary distinctions of the pre-*Katz* era, such that privacy tends to be conceptualized as "a discrete commodity, possessed absolutely or not at all."[78] Although couched as a contextual analysis, the *Katz* standard remains persistently bound to physical seclusion and concealment. What is reasonable "under the circumstances"[79] is nearly always to maintain absolute obscurity, from both the government and the public generally. As applied to tangible objects in the terrestrial domain, seclusion is correlated with the right to exclude and thus remains centralized around property rights and physical intrusion.[80] But

---

at least until the latter half of the 20th century." (citing Kyllo v. United States, 533 U.S. 27, 31 (2001))); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1244–46 (2012) (observing that Fourth Amendment doctrine is grounded in property concepts); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) (referencing the historical connection between Fourth Amendment protections and trespass upon property).

72. Katz v. United States, 389 U.S. 347, 350–51 (1967).

73. *Id.* at 351.

74. *Id.* at 350–51.

75. *Id.* at 360 (Harlan, J., concurring); *see also Carpenter*, 138 S. Ct. at 2213–14 (discussing the *Katz* approach).

76. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

77. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2213–14 (discussing the *Katz* reasonable expectation of privacy standard).

78. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

79. *Katz*, 389 U.S. at 355 (quoting Berger v. New York, 388 U.S. 41, 57 (1967)).

80. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society. One of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude. Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest. These ideas were rejected both in *Jones* and *Katz*. But by focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment." (citations omitted)); *see also* Oliver v. United States, 466 U.S. 170, 183–84 (1984). In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the majority opinion and each of the four dissenting opinions reaffirmed the connection between Fourth Amendment protections and trespass-upon-property. *See Carpenter*, 138 S. Ct. at 2213–14; *id.* at 2227 (Kennedy, J., dissenting) ("*Katz* did not abandon reliance on property-based concepts."); *id.* at 2235–36 (Thomas, J., dissenting) (rejecting

even here, mere seclusion is not always sufficient. In certain circumstances, physical trespass across property lines is permitted without triggering a Fourth Amendment search, even where the property owner has taken significant efforts to deter others from accessing the area.[81] Likewise, many invasive technologies that permit the government to gain information from secluded areas beyond the property line do not constitute a trespass or intrusion at all.[82]

The failure of seclusion, whether by property interest or physical barriers, places far greater pressure on concealment to secure one's privacy interest. The Supreme Court's 1986 decision in *California v. Ciraolo*[83] demonstrates this point. Ciraolo maintained a marijuana garden in his yard, closely adjacent to his home.[84] His yard was completely enclosed by a six-foot outer fence, and the marijuana garden itself was enclosed within a second, ten-foot inner fence.[85] As a result, the garden was entirely obscured from ground-level observation.[86] Undeterred, local police "secured a private plane and flew over [Ciraolo's] house at an altitude of 1,000 feet,"[87] from which they observed and photographed the marijuana plants growing below.[88] The Court held that no search had occurred in this case because Ciraolo's clear subjective expectation of privacy, evidenced by seclusion of the marijuana behind multiple tall fences,[89] was not one that society was willing to recognize as legitimate.[90] Although cast as a test of contextual reasonableness, this conclusion is grounded firstly in bright-line distinctions between concealment and disclosure.

As the Court observed in *Katz*, "[W]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[91] Public exposure is in turn defined not by reference to active

---

Katz in favor of a property-based approach); *id.* at 2260 (Alito, J., dissenting) (characterizing *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), as turning on the defendants' lack of property rights in the property of another); *id.* at 2267–71 (Gorsuch, J., dissenting) (suggesting that a return to property concepts might resolve difficulties arising in regards to the third-party doctrine).

81. *See, e.g.*, United States v. Dunn, 480 U.S. 294, 296 (1987) (holding that erecting multiple ranch style fences across an open field does not create an expectation of privacy); Oliver v. United States, 466 U.S. 170, 181 (1984) (holding that erecting fences and "No Trespassing" signs, even on secluded land, did not create an expectation of privacy in an open field).

82. *See, e.g.*, Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986) (holding that aerial photographs taken using a standard precision aerial mapping camera did not constitute a search, even where the target used elaborate security around the perimeter to entirely obscure ground-level views); California v. Ciraolo, 476 U.S. 207, 214 (1986) (holding that aerial observation of a fenced-in backyard within the curtilage of a home did not constitute a search).

83. 476 U.S. 207 (1986).

84. *Ciraolo*, 476 U.S. at 213.

85. *Id.* at 209.

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.* at 211.

90. *Id.* at 214.

91. Katz v. United States, 389 U.S. 347, 351 (1967). *But see* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (indicating, without full elaboration, that this is not a per se rule, as "[a] person

disclosure or the reasonableness of one's efforts to maintain practical obscurity through seclusion but rather by near-perfect concealment. Whatever law enforcement is able to observe from a vantage point to which they have legal access[92]—whether by crossing open fields surrounded by fencing,[93] by peering through a small knothole in a tall fence,[94] or by hiring a small plane to fly through unrestricted airspace[95]—has been exposed to the public and thus loses all protection under the Fourth Amendment. In the absence of complete and total concealment, the individual is said to assume the risk that the government will gain access to even the most secluded areas, even if by extraordinary or unexpected means.[96]

This assumption of risk rationale is applied to "intangible" information in a second, related line of cases involving the disclosure of information to undercover and confidential informants.[97] These informant cases place the dominance of the concealment-disclosure distinction in sharp relief. For just as considerable efforts to seclude tangible property have often proven legally insufficient in the absence of absolute concealment, only absolute silence ensures the maintenance of one's privacy interest in information. The Court has repeatedly held that you rarely enjoy a reasonable expectation of privacy in your oral communications with another, even a trusted associate or a false friend,[98] as you necessarily assume the risk that your confidence will be betrayed.[99] As the Court remarked in *United States v. White*,[100] "however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected,"[101]

---

does not surrender all Fourth Amendment protection by venturing into the public sphere").

92. *Ciraolo*, 476 U.S. at 213 ("[T]he mere fact that an individual has taken measures to restrict some views of his activities [does not] preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible." (citing United States v. Knotts, 460 U.S. 276, 282 (1983))).

93. United States v. Dunn, 480 U.S. 294, 303–04 (1987); Oliver v. United States, 466 U.S. 170, 179–80 (1984).

94. *Ciraolo*, 476 U.S. at 210 (discussing with approval California's analogy between overflight and observation through "a knothole or opening in a fence").

95. *Id.* at 213–14.

96. *Id.* at 211–14 (finding no reasonable expectation of privacy where a ten-foot fence surrounding marijuana plants on private property "might not shield these plants from the eyes of a citizen or a policeman perched on the top of a truck or a two-level bus").

97. *See* United States v. White, 401 U.S. 745, 749 (1971) (holding that the defendant assumed the risk that his companions might share the content of their conversations with police, even by radio transmitter); Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding that the defendant assumed the risk that his companions might share the content of their conversations with police and testify as to that content); Lopez v. United States, 373 U.S. 427, 438–40 (1963) (holding that the defendant assumed the risk that his companions might share the content of their conversations with police, including by using a hidden recording device).

98. On Lee v. United States, 343 U.S. 747, 753–54 (1952) (finding no Fourth Amendment violation where defendant was simply "talking . . . indiscreetly with one he trusted").

99. *Hoffa*, 385 U.S. at 302 ("[T]he Fourth Amendment [does not] protect[] a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

100. 401 U.S. 745 (1971).

101. *White*, 401 U.S. at 749.

as the Fourth Amendment simply does not credit "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[102] Once again, attempts at seclusion—in the form of physical barriers (meeting in a home or office) and restricted access (limiting oneself to close confidants)—have proven insufficient to establish a legitimate privacy interest.[103] Only absolute concealment through absolute silence will suffice.[104]

B. The Third-Party Doctrine

The third-party doctrine emerged from two strands of Fourth Amendment jurisprudence—the public exposure cases[105] and the informant cases[106]—both of which developed prior to *Katz* but survived the transition from spatial privacy to protections grounded in one's reasonable expectation of privacy.[107] Indeed, *Katz* made this connection explicitly. First, the Court enunciated the rule at the heart of the third-party doctrine: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[108] Second, the Court supported this assertion with citations to two cases: *United States v. Lee*,[109] a public exposure case involving the observation of contraband visible on the deck of a boat at sea,[110] and *Lewis v. United States*,[111] an informant case involving an undercover agent invited into the defendant's home.[112]

The Court affirmed this approach just four years later in *White*, in which it confirmed the continuing validity of its informant jurisprudence post-*Katz*.[113] Defendant White sought to exclude the testimony of government agents regarding the content of conversations between himself and a cooperating informant, including at least one conversation that took place within White's

---

102. *Hoffa*, 385 U.S. at 302.

103. *See, e.g.*, *White*, 401 U.S. at 747 (finding no legitimate privacy interest where a government informant brought a radio transmitter into the defendant's home and automobile); *Hoffa*, 385 U.S. at 301–02 (finding that seclusion within a constitutionally protected physical area does not create a legitimate privacy interest in conversations with a third-party cooperating witness, even where that witness could be characterized as a close confidant).

104. *See, e.g.*, *White*, 401 U.S. at 762–65 (Douglas, J., dissenting) (describing the chilling effect of the third-party doctrine and the assumption of risk rationale).

105. *See* Kerr, *Third-Party Doctrine*, *supra* note 21, at 570–71 (discussing the exposure aspect of the third-party doctrine).

106. *See id.* at 567–69 (discussing the informant cases); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 266–67 (2016) (same).

107. Tokson, *Automation*, *supra* note 12, at 598; *see also White*, 401 U.S. at 749 (holding that these cases were "left undisturbed by *Katz*").

108. Katz v. United States, 389 U.S. 347, 351 (1967).

109. 274 U.S. 559 (1927).

110. *See Lee*, 274 U.S. at 563.

111. 385 U.S. 206 (1966).

112. *See Lewis*, 385 U.S. at 206–07.

113. United States v. White, 401 U.S. 745, 750 (1971).

home.[114] The Court held that White's expectation of privacy in any information shared with a third party was not justified[115] and that White had assumed the risk that the informant might share the content of their conversations with police.[116] Thus, by failing to maintain absolute concealment through absolute silence, White had obviated any legitimate privacy interest in the information that he revealed.

These basic principles would serve as the foundation of the modern third-party doctrine, which allows the government to obtain information from third parties without first procuring a search warrant.[117] In the first of two leading cases, *United States v. Miller*,[118] the Court upheld the use of a third-party subpoena to obtain the bank records of the defendant.[119] Starting from the basic proposition in *Katz*—that information exposed to the public is no longer protected by the Fourth Amendment[120]—the Court found no reasonable expectation of privacy in "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[121] Relying on the informant cases, the Court concluded that Miller "[took] the risk, in revealing his affairs to another, that the information would be conveyed by that person to the Government,"[122] even where the information was revealed only for a limited purpose.[123] Here, the information provided to the government included deposit slips, checks, and account statements[124]—documents used by the account holder primarily to facilitate transactions with third parties and to manage the financial aspects of business operations.[125] Although the account holder maintained an independent relationship with the bank, these documents primarily related to these external concerns. The bank acted, in essence, as a transactional intermediary.[126]

---

114. *Id.* at 746–47.

115. *Id.* at 749.

116. *Id.* at 752.

117. *See* Kerr, *Third-Party Doctrine*, *supra* note 21, at 563 ("By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed.").

118. 425 U.S. 435 (1976).

119. *Miller*, 425 U.S. at 436–37.

120. Katz v. United States, 389 U.S. 347, 351 (1967).

121. *Miller*, 425 U.S. at 442.

122. *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971)); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (describing *Miller*'s reliance on an assumption of risk rationale).

123. *Miller*, 425 U.S. at 443 (confirming that the third-party doctrine applies "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed" (first citing *White*, 401 U.S. at 752; then citing Hoffa v. United States, 385 U.S. 293, 302 (1966); and then citing Lopez v. United States, 373 U.S. 427 (1963))).

124. *Id.* at 438.

125. *See id.* at 448 (Brennan, J., dissenting) (noting that the records in question were "transmit[ted] to the bank in the course of his business operations" (quoting Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974))).

126. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 41 (2007) (describing the bank employees in *Miller* as "human intermediaries").

The second of these cases, *Smith v. Maryland*,[127] applied this same approach to a form of "intangible" information.[128] Smith was suspected in a robbery and stalking incident, wherein someone made threatening and obscene phone calls to the victim.[129] At the request of police, but without a warrant, "the telephone company . . . installed a pen register at its central offices to record the numbers dialed from the telephone at [Smith's] home."[130] Prior to trial, Smith unsuccessfully "sought to suppress 'all fruits derived from the pen register' on the ground that the police had failed to secure a warrant prior to its installation."[131] Affirming the denial of Smith's motion to suppress, the Supreme Court held that Smith had no reasonable expectation of privacy in the numbers dialed because, as established by *Miller* and its predecessors, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[132] But *Smith* extended this binary rule of absolute concealment to automated transactions that are highly unlikely to ever involve a human being, whether as a practical matter and/or because such access is contractually disclaimed. Thus, the third-party doctrine is triggered by the disclosure of information that occurs whenever an individual voluntarily interacts with an automated third-party processing system,[133] where there is even the faintest possibility of human observation.[134]

II. THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

Smith remains the Supreme Court's most definitive statement on the application of the third-party doctrine to electronic communications and related technologies. Yet it was issued nearly forty years ago, at the leading edge of the digital age. In several key respects, *Smith* presaged the coming transformation of the information environment, applying the third-party doctrine to the transmission of information by an automated system—owned and operated by a private intermediary—that collects, processes, and stores associated data. But the *Smith* Court could not have possibly imagined the speed and scale of the coming advancements in computer and information technologies nor the challenges these developments would present for the Court's "modern" third-party doctrine. In this Section, I address two advancements in particular: the initial shift to digitized electronic communications and the move to cloud computing.

---

127. 442 U.S. 735 (1979).

128. *Smith*, 442 U.S. at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)) (addressing the search and seizure of telephone numbers dialed, rather than physical documents or contents of conversations).

129. *Id.* at 737.

130. *Id.*

131. *Id.*

132. *Id.* at 743–44.

133. *Id.* at 744–45 (declining "to hold that a different constitutional result is required because the telephone company has decided to automate").

134. *See* Tokson, *Automation*, *supra* note 12, at 600 (discussing the conflict between the automation rationale and the human-observer theory of the third-party doctrine).

The transition from analog to digitized electronic communication,[135] such as email,[136] created a gap in privacy regulation that left personal communications vulnerable both to interception during transmission and to retrieval from the storage facilities of the sender, recipient, or service provider.[137] Tasked by Congress in the mid-1980s to investigate potential privacy concerns related to these new electronic communication and surveillance technologies,[138] the Office of Technology Assessment (OTA) concluded that neither the existing statutory protections nor judicial interpretations of the Fourth Amendment were adequate to safeguard individual privacy interests.[139] Of particular relevance here, the OTA expressed concern that application of the third-party doctrine—holding that there is no reasonable expectation of privacy in information revealed or voluntarily conveyed to a third party[140]—might well extinguish Fourth Amendment protections for stored electronic communications.[141]

This led Congress to enact the Electronic Communications Privacy Act of 1986 (ECPA),[142] which extended existing statutory restrictions on the use of traditional wiretaps to the interception of electronic data transmissions[143] while placing lesser restrictions on government access to both the content of stored electronic communications[144] and the data provided to third-party remote-computing services for storage and processing.[145] In the three decades since the passage of the ECPA, however, these statutory protections have come under increasing criticism.[146] Law enforcement has taken advantage of a dramatic increase in remote storage capabilities to avoid the more onerous requirements of the ECPA's wiretap provisions by instead "accessing stored electronic

135. *See* OFFICE OF TECH. ASSESSMENT, *supra* note 11, at 13 (discussing the emergence of digital communications, focusing on email and cell phones).

136. *See id.* at 46–47 (describing the growing popularity and commercialization of email); Raphael Cohen-Almagor, *Internet History*, INT'L J. TECHNOETHICS, Apr.–June 2011, at 45, 53 (same). Ray Tomlinson is widely credited with introducing email when he created the first "basic email message send-and-read software" in 1972. Barry M. Leiner et al., *The Past and Future History of the Internet*, COMM. ACM, Feb. 1997, at 102, 103.

137. OFFICE OF TECH. ASSESSMENT, *supra* note 11, at 48–50 (describing multiple points of email vulnerability).

138. *See id.* at 3–4.

139. *Id.* at 10.

140. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

141. *See* OFFICE OF TECH. ASSESSMENT, *supra* note 11, at 50 (stating that "[e]xisting law offers little protection" for stored communications vulnerable to interception by third parties).

142. Pub. L. No. 99-508, 100 Stat. 1848 (current version in scattered sections of 18 U.S.C.).

143. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 2 (2015).

144. *Id.* at 3–5.

145. *Id.*

146. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 386–90 (2014) (discussing current criticisms of the ECPA); Raquel, *supra* note 19, at 490 (calling the ECPA "painfully outdated").

communications, such as emails, directly from a service provider."[147] In many cases, the Stored Communications Act (SCA), which governs such access, waives the more stringent warrant requirement in favor of a subpoena or court order,[148] raising privacy concerns.[149]

The "cloud computing revolution"[150] amplifies and extends the gap in online privacy law protections identified by the OTA. In a typical cloud computing system, some combination of computing resources ("e.g., networks, servers, storage, applications, and services") is outsourced to a third party, which owns, manages, and operates those systems.[151] Core software applications and all associated data—whether encompassed in the communication from user to user, or created and collected in the course of that interaction with the system—may be maintained entirely on external facilities under the control of the provider.[152] Email services provide an excellent example of this model. The Google web-based email service Gmail, for instance, operates on a cloud computing Software-as-a-Service model.[153] The email application, user's emails, and all associated data reside on Google's remote servers and are accessible by the user

147. THOMPSON II & COLE, *supra* note 143, at 3; *accord* Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2018).

148. THOMPSON II & COLE, *supra* note 143, at 3.

149. *See* Raquel, *supra* note 19, at 482–85 (describing the various circumstances and mechanisms for compelled governmental access, providing protections that fall well short of constitutional safeguards).

150. *E.g.*, Timothy J. Calloway, *Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm?*, 11 DUKE L. & TECH. REV. 163, 174 (2012) (utilizing the phrase "cloud computing revolution"). According to the technology research firm Gartner, Inc., the total public cloud services market—including Cloud Business Process Services (BPaaS), Cloud Application Infrastructure Services (PaaS), Cloud Application Services (SaaS), Cloud Management and Security Services, and Cloud System Infrastructure Services (IaaS)—brought in an estimated $153.5 billion in revenue in 2017. *Gartner Forecasts Worldwide Public Cloud Revenue To Grow 21.4 Percent in 2018*, GARTNER, INC. (Apr. 12, 2018), https://www.gartner.com/newsroom/id/3871416 [perma.cc/V8RQ-K3TC]. Gartner forecasts the overall market to reach $302 billion by 2021. *Id.*

151. *See* PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., SP800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf [perma.cc/V8RQ-K3TC] (noting that the National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"); *see also* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43015, CLOUD COMPUTING: CONSTITUTIONAL AND STATUTORY PRIVACY PROTECTIONS 1 (2013) [hereinafter THOMPSON II, CLOUD COMPUTING] (observing that cloud computing allows users to manipulate data over the internet on a third-party computer, rather than on their own computer).

152. *See* David W. Opderbeck, *Encryption Policy and Law Enforcement in the Cloud*, 49 CONN. L. REV. 1657, 1671–72 (2017) (describing the cloud-based nature of most email systems, as well as the migration of documents associated with productivity software (e.g., Word, PowerPoint, and Excel) to cloud-based platforms).

153. *Id.* (reviewing the various services utilizing the SaaS model). The SaaS model is generally designed to perform certain functions or tasks. *Id.* For example, with G Suite, Google offers "a set of word processing, presentation, spreadsheet and other productivity tools." *Id.* Microsoft's Office suite products now similarly function on a SaaS model. *Id.*

via web browser or program interface. Cloud storage services, such as Dropbox, are functionally similar.[154] Dropbox utilizes user-downloaded software applications to automatically transfer copies of a user's documents and other computer files to the service's remote cloud servers.[155] These files are synced across the user's computers and mobile devices, each interacting with the Dropbox servers, creating multiple copies in multiple locations.[156]

From a Fourth Amendment perspective, cloud-computing systems share several key characteristics. First, they are a distributed computing model with components spread across a multitude of facilities owned and/or operated by private third parties.[157] Second, these automated third-party services are designed to actively solicit and passively collect, store, generate, utilize, and analyze "vast quantities of personal data."[158] Some of that data is provided by the user and some is created as a product of system operations, with the latter often derived from user-provided content.[159] Third, this information is collected, generated, stored, and analyzed in the context of a commercial relationship and in furtherance of "a variety of legitimate business purposes."[160] Fourth, the rapid growth of cloud-computing facilities allows for the wholesale migration of computer systems and essential services to third-party providers,[161] significantly expanding both the quantity and range of information entrusted to third-party providers.[162] Finally, cloud-computing systems and associated data practices are now nearly impossible to avoid in the course of meaningful social and economic

154. *See* Erik C. Shallman, Comment, *Up in the Air: Clarifying Cloud Storage Protections*, 19 INTELL. PROP. L. BULL. 49, 50 (2014) (describing Dropbox as a cloud storage service).

155. *Id.*

156. *See id.* (noting that a saved file can be accessed from any computer with internet access).

157. *See* Shawish & Salama, *supra* note 16, at 41, 63 (observing that "Cloud Computing shifts the computation from local, individual devices to distributed, virtual, and scalable resources" and involves "massive use of third-party services and infrastructures . . . to host important data and to perform critical operations")

158. Tokson, *Automation*, *supra* note 12, at 604.

159. *See* Jared A. Harshbarger, *Cloud Computing Providers and Data Security Law: Building Trust with United States Companies*, 16 J. TECH. L. & POL'Y 229, 231–32 (2011) (describing cloud-based data storage and processing, utilizing data provided by the user, data processing by the service, and data created through those processes).

160. Smith v. Maryland, 442 U.S. 735, 743 (1979).

161. Cloud computing services are commonly divided into three categories: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS). Raquel, *supra* note 19, at 473. The IaaS model, in particular, allows users to offload their *entire* computer infrastructure to a flexible virtual machine that emulates a computer system, but actually resides in enormous data centers. *See* Shawish & Salama, *supra* note 16, at 49–50. With an IaaS model, all of the user's software systems and associated data, including both raw data and data analytics, are generally stored on third-party computing facilities. *Id.*

162. *See* Issacharoff & Wirshba, *supra* note 13, at 993 ("[T]he growth of 'cloud storage' subjects significantly more private data to the third party exception."); Raquel, *supra* note 19, at 469 (describing cloud computing as "a transformative computing model" that places information once held by individuals on to "remote servers owned or operated by third parties"); *see also* United States v. Cotterman, 709 F.3d 952, 965 (9th Cir. 2013) ("With the ubiquity of cloud computing, the government's reach into private data becomes even more problematic.").

engagement with modern daily life.[163]

In sharp contrast to this model of ubiquitously distributed computing and data flows, the Fourth Amendment remains stubbornly focused on one's ability to conceal and control access to personal information. Information disclosed to a third party, even an automated system with little chance of human observation,[164] generally no longer enjoys Fourth Amendment protections.[165] It is an "approach . . . ill suited to the digital age,"[166] in which "the third-party doctrine has become a greedy exception that leaves little room over for the Fourth Amendment."[167] Congress struggles to legislate even the most targeted exceptions,[168] while courts strain to analogize the postal service of 1877[169] to modern communication via email[170] or text message.[171] But as Chief Justice Roberts observed in *Riley v. California*,[172] strained analogies often "crumble[] entirely" when applied to cloud computing.[173]

---

163. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[P]eople reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."); *see also* Riley v. California, 134 S. Ct. 2473, 2484 (2014) (describing modern cell phones as "a pervasive and insistent part of daily life").

164. Tokson, *Automation*, *supra* note 12, at 600 (discussing the conflict between the automation rationale and the human-observer theory of the third-party doctrine).

165. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (stating that under the third-party doctrine, "an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" (first citing Smith v. Maryland, 442 U.S. 735, 742 (1979); then citing United States v. Miller, 425 U.S. 435, 443 (1976))).

166. *Id.*; *see also* Bedi, *Facebook*, *supra* note 19, at 19–28 (reviewing various criticisms of the Fourth Amendment and third-party doctrine); Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1475–80 (2017) (describing the Supreme Court's recent recognition of the lag between privacy law and social-technical practices, including cloud computing); Couillard, *supra* note 60, at 2218 (discussing both the emerging Fourth Amendment jurisprudence regarding email and other forms of communication, as well as the difficulties of applying existing principles to cloud computing).

167. Bryan H. Choi, *For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence*, 37 CARDOZO L. REV. 185, 217 (2015); *see also* Monu Bedi, *Social Networks, Government Surveillance, and the Fourth Amendment Mosaic Theory*, 94 B.U. L. REV. 1809, 1814 (2014) (arguing that, "[u]nder a strict application of [third-party] doctrine," no internet communications "merit Fourth Amendment protection" because they "are housed in . . . proprietary systems for various periods of time in order to facilitate the transmission").

168. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 23–25 (2014) (discussing legislation intended to restore, to a certain degree, privacy protections lost by application of the third-party doctrine).

169. *Ex parte* Jackson, 96 U.S. 727, 733 (1878) (prohibiting government officials from intercepting and examining the content of sealed letters in the U.S. mail, unless they first obtain a warrant).

170. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 285–88 (6th Cir. 2010) (discussing *Ex parte Jackson*). *But see* United States v. Ackerman, 831 F.3d 1292, 1304–05 (10th Cir. 2016) (discussing the unsettled nature of the issue).

171. *See, e.g.*, Love v. State, 543 S.W.3d 835, 842–45 (Tex. Crim. App. 2016) (discussing *Ex parte Jackson* and reviewing cases analogizing text messages to the content of an envelope conveyed through the U.S. mail).

172. 134 S. Ct. 2473 (2014).

173. *Riley*, 134 S. Ct. at 2491 (defining cloud computing as "the capacity of Internet-connected

In the absence of clear limitations on the third-party doctrine, it seems the classic case of an exception that threatens to swallow the rule. As Eleventh Circuit Judge Beverly Martin recently warned:

> [B]lunt application of the third-party doctrine threatens to allow the government access to a staggering amount of information that surely must be protected under the Fourth Amendment . . . . [B]y allowing a third-party company access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information.
>
> And why stop there? Nearly every website collects information about what we do when we visit. [Broad application of the third-party doctrine] allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we "friend," or Amazon.com what we buy, or Wikipedia.com [sic] what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask "cloud"-based file-sharing services like Dropbox or Apple's iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this.[174]

Although there is precious little case law addressing the application of the third-party doctrine to these networked technologies, there are certainly indications that Judge Martin's concerns are well founded. As Laura Donohue has observed, the Supreme Court "has been slow to recognize a Fourth Amendment interest in *digital* communications," and "the lower courts remain divided" on many key applications—including protections for the content of both email and text messages.[175] And as Justice Gorsuch recently observed, the Supreme Court's binary approach to the third-party doctrine leads to potentially untenable results.

> The problem isn't with the [lower court's] application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely.[176]

But are such results really so unlikely? In one recent case in which the government sought "essentially . . . every posting and action . . . taken through Facebook,"[177] a New York court held that "under the Third-Party Doctrine only a subpoena and prior notice (a much lower hurdle than probable cause) are

devices to display data stored on remote servers rather than on the device itself"). Interestingly, Chief Justice Roberts suggested, without so deciding, that for Fourth Amendment purposes it "generally makes little difference" whether data is stored locally or in the cloud. *Id.*

174. United States v. Davis, 785 F.3d 498, 535–36 (11th Cir. 2015) (Martin, J., dissenting).

175. Donohue, *Digital World*, *supra* note 1, at 651–56.

176. Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

177. *In re* 381 Search Warrants Directed to Facebook, Inc., 14 N.Y.S.3d 23, 24 (App. Div. 2015), *aff'd* 78 N.E.3d 141 (N.Y. 2017).

needed to compel an ISP to disclose the contents of an email or of files stored on a server."[178] To borrow the words of Judge Martin, "I am convinced that most internet users would be shocked by this."[179]

III. A PROPOSAL FOR LIMITING THE THIRD-PARTY DOCTRINE

My proposal for limiting the reach of the third-party doctrine proceeds in three parts. In Part III.A, I argue that our constitutional commitment to freedom of thought is historically and properly connected to the enumeration of "papers" as a distinct object of Fourth Amendment protection. This Part begins with an explication of freedom of thought, primarily as an aspect of First Amendment doctrine. I then turn to the relationship between freedom of thought and privacy rights, including the relevance of certain core Fourth Amendment principles, with a focus on the link between protections for personal papers and autonomous thought.

In Part III.B, I seek to revive the connection between freedom of thought and personal papers. I begin by exploring various models of cognition and the role of cognitive artifacts in these processes and systems. I then explain how papers and their digital equivalents serve as cognitive artifacts capable of representing and storing information, and thus function as integral components of a cognitive system performing cognitive tasks. Although conceptualized through the lens of contemporary cognitive science, this account is consistent with historical protections for personal papers, translating the intuition of prior generations into current cognitive theory.

In Part III.C, I propose changes to the third-party doctrine intended to reestablish enhanced constitutional protections for papers and their digital equivalents when functioning as cognitive artifacts. In the emerging information environment, these cognitive artifacts are no longer confined within protected spaces and personal confidences but are now distributed across automated third-party networks that store, process, and transfer the information. Yet they remain integral components of our cognitive processes. Indeed, there is good reason to conclude that our ability to readily access and incorporate vast stores of information maintained, represented, stored, and even operated upon by cognitive artifacts—as well as, consequently, our growing reliance on these components of information processing—has only reinforced the role of these artifacts in human cognition. By this account, in which papers are recognized and valued as cognitive artifacts, our constitutional commitment to freedom of thought compels modifications to the third-party doctrine to restore certain Fourth Amendment protections.

A. Freedom of Thought, Privacy of Thought, and Fourth Amendment Papers

The Supreme Court has consistently recognized the central importance of

178. *Id.* at 21 (issue not addressed on appeal).

179. *Davis*, 785 F.3d at 536 (Martin, J., dissenting).

protecting individual freedom of thought from government interference.[180] It "was first recognized by the Supreme Court in . . . 1878," in the context of religious belief,[181] and in secular matters "by Justices Holmes and Brandeis as part of their dissenting tradition in free speech cases in the 1910s and 1920s."[182] In 1937, Justice Cardozo referred to freedom of thought as "the matrix, the indispensable condition, of nearly every other form of freedom."[183] In 1969, Justice Marshall wrote that "[o]ur whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[184] And in 2002, Justice Kennedy declared that "[t]he right to think is the beginning of freedom."[185] Yet, despite this history, the Court has remained largely noncommittal as to the constitutional foundations and substance of this "most vital of our liberties."[186]

Freedom of thought is most often framed by its relationship to the First Amendment.[187] Thomas Jefferson, for instance, wrote of the importance of "the rights of thinking, and publishing our thoughts by speaking or writing."[188] In the narrower form of this conception, freedom of thought is regarded for its instrumental value in promoting the outwardly expressive liberties of speech, association, assembly, and free exercise.[189] In its more expansive form, freedom of thought is imbued with the intrinsic value of individual autonomy and integrity.[190] In some respects, these different conceptions of freedom of thought parallel differing views of First Amendment protections for free expression. Thus, by exploring the asserted values of free expression, we gain insight into the substance of freedom of thought.

Protections for free expression are generally justified by reference to one of three values: promotion of democratic self-governance, the pursuit of truth, or the preservation of individual autonomy and self-realization.[191] The first of these

---

180. *See, e.g.*, Ashcroft v. Free Speech Coal., 535 U.S. 234, 253 (2002) ("The government 'cannot constitutionally premise legislation on the desirability of controlling a person's private thoughts.'" (quoting Stanley v. Georgia, 394 U.S. 557, 566 (1969))); Kovacs v. Cooper, 336 U.S. 77, 97 (1949) (Frankfurter, J., concurring) ("[W]ithout freedom of thought there can be no free society."); Doe v. City of Lafayette, 377 F.3d 757, 777 (7th Cir. 2004) ("[F]reedom of the mind occupies a highly-protected position in our constitutional heritage."); Richards, *Intellectual Privacy*, *supra* note 37, at 412 ("The Supreme Court has repeatedly declared that the constitutional guarantee of freedom of thought is at the foundation of what it means to be a free society.").

181. Richards, *Intellectual Privacy*, *supra* note 37, at 410 (citing Reynolds v. United States, 98 U.S. 145 (1878)).

182. *Id.*

183. Palko v. Connecticut, 302 U.S. 319, 326–27 (1937).

184. Stanley v. Georgia, 394 U.S. 557, 565 (1969).

185. Ashcroft v. Free Speech Coal., 535 U.S. 234, 253 (2002).

186. Richards, *Intellectual Privacy*, *supra* note 37, at 388–89.

187. *See, e.g.*, *id.*

188. Thomas Jefferson, *Letter to David Humphreys*, *in* 5 THE WRITINGS OF THOMAS JEFFERSON 86, 90 (Paul Leicester Ford ed., 1895).

189. *See* Kolber, *supra* note 41, at 1387–88.

190. *See* Tuchman, *supra* note 47, at 2280.

191. *See* David S. Han, *Autobiographical Lies and the First Amendment's Protection of Self-Defining Speech*, 87 N.Y.U. L. REV. 70, 89–93 (2012) ("[T]hree general rationales are most commonly

values is distinctly instrumental in nature, presenting free expression as a necessary condition for the realization of democratic self-governance.[192] This approach preferences both certain forms of expression (public discourse and deliberation) and certain topics (political speech) as worthy of greater protection.[193] The second of these values justifies protections for free expression as instrumental to the pursuit of truth[194]—but a sort of public truth. In this context, free expression is valued as a necessary condition to the development and maintenance of a "marketplace of ideas," in which competing theories and opinions are tested, and from which *the* truth is likely to emerge.[195] The third value, preservation of individual autonomy and self-realization,[196] is different in kind from these first two values. Apart from the promotion of public values such as democratic self-governance or realization of a public truth, this account is unmistakably focused on the individual, with derivative benefits to society at large. Free expression is instrumentally valued as "an integral part of the development of ideas, of mental exploration and of the affirmation of self,"[197] fostering "individual self-realization and self-determination"[198]—a personal truth. These instrumental values are closely tied to the intrinsic value of free expression as "an essential attribute of individual personhood."[199] Thus, speech "receive[s] constitutional protection (at least in part) as [an] embodiment[] of collective respect for individual liberty or autonomy."[200]

Freedom of thought implicates many of these same concerns as to justification, value, and substance. Adam Kolber, for instance, began with what he referred to as a distinction between the "intertwined" and "independent" views of freedom of thought.[201] Specifically, he asked "whether the First Amendment protects thought itself . . . or only protects thought when it is linked to expression."[202] Under the intertwined view, "freedom of thought holds only instrumental value from a First Amendment perspective . . . as a way of

---

advanced as bases for the First Amendment's protection of free speech: the pursuit of truth, the promotion of democratic self-government, and the preservation of individual autonomy and self-realization.").

192. *See id.* at 91; *see also* Leora Harpaz, *Justice Jackson's Flag Salute Legacy: The Supreme Court Struggles To Protect Intellectual Individualism*, 64 TEX. L. REV. 817, 826 n.34 (1986) (citing various adherents to the instrumental and intrinsic theories of the First Amendment).

193. *See* Han, *supra* note 191, at 91.

194. *Id.* at 90.

195. *Id.* (quoting Abrams v. United States, 250 U.S. 616, 630 (1919) (Holmes, J., dissenting)).

196. *Id.* at 92–93.

197. Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963).

198. C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 UCLA L. REV. 964, 966 (1978).

199. *See* Han, *supra* note 191, at 92.

200. C. Edwin Baker, *Private Power, the Press, and the Constitution*, 10 CONST. COMMENT. 421, 436 (1993).

201. Kolber, *supra* note 41, at 1383.

202. *Id.*

promoting expression."[203] In an absence of "a connection to expression," "freedom of thought holds only modest value."[204] This narrow focus on the instrumental value of freedom of thought has the benefit of reinforcing consistency with theories of free expression, but it potentially suffers from the implicit limitations of those views (e.g., public discourse and deliberation, the search for a public truth, and elevated protections for political speech). The independent view, on the other hand, "protects freedom of thought even in cases that lack recognized forms of expression."[205] Kolber recognized two potential supporting theories for this view. The first is simply that the First Amendment "values thought separately from expression."[206] The second is that, even if "thought is only instrumentally valuable from a First Amendment perspective[,] . . . the connection between thought and expression [is] so close and important that we need not find expression in any particular case."[207]

Until recently, these contested accounts of freedom of thought have generally eluded resolution because resolution has never been required.[208] The purely internal workings of our minds are locked within flesh and bone, beyond penetration and without the need for legal protections.[209] As Marc Jonathan Blitz has observed, freedom of thought has been invoked "not as a means for protecting our *already protected* internal mental freedom, but rather as a justification for shielding certain *external* actions . . . that many view as having a close connection to, or providing indispensable support for, our capacity to think freely and autonomously."[210]

> The Supreme Court, for example, has invoked freedom of thought in cases barring the government from penalizing us for joining, or refusing to join, certain political groups, for refusing to affirm certain government-mandated messages or commitments (in loyalty oaths, flag salutes, or license plates), or for watching an obscene film in our own home. All of these activities are performed in the external world, not in the realm of pure fantasy or imagination. But the Court held that punishing them was tantamount to punishing thought.[211]

Freedom of thought has thus been protected from external sources of government interference with respect to the information we receive, disseminate, adopt, and discuss with nongovernmental actors. Likewise, the government may act to preserve freedom of thought from excessive external interference by others. As Justice Frankfurter observed in *Kovacs v. Cooper*,[212] the legislature

---

203. *Id.* at 1386.

204. *Id.*

205. *Id.* at 1386–87.

206. *Id.* at 1387.

207. *Id.*

208. *See* Blitz, *Intellectual Privacy*, *supra* note 42, at 15.

209. *See id.* ("[W]e hardly need constitutional protection, or any other type of legal wall, to insulate an activity—like purely mental activity—that is *already* fully insulated by nature.").

210. *Id.* (footnote omitted).

211. *Id.* at 15–16 (footnotes omitted).

212. 336 U.S. 77 (1949).

may impose reasonable restrictions intended to "safeguard[] the steadily narrowing opportunities for serenity and reflection[, for] [w]ithout such opportunities freedom of thought becomes a mocking phrase, and without freedom of thought there can be no free society."[213]

This focus on external interference underscores the importance of distinguishing between the object of protection and the conditions necessary for its protection. Seana Shiffrin, for instance, identified the object of protection as "the *process* by which ideas and expressions are generated, nurtured, and mooted, both in individuals and within groups."[214] Shiffrin then described the conditions necessary to realize this value:

> The autonomous agent must have some ability to control what influences she is exposed to, to what subjects she directs her mind, and whether she, at all times, directs her mind toward anything at all or instead "spaces out" and allows the mind to relax and wander. To function as an independent thinker and evaluator, the individual must have domains in which she may enjoy the privacy of her thoughts.[215]

Thus, just as "individual freedom of thought is a clear requisite for meaningful freedom of speech protections,"[216] so too is privacy of thought regarded as a necessary condition for freedom of thought.[217]

Neil Richards similarly observed that "the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants,"[218] systematizing many of these various threads under a theory of what he terms "intellectual privacy."[219]

> Intellectual privacy is the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others . . . . The ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy. In this way, intellectual privacy is a cornerstone of meaningful First Amendment liberties.[220]

Richards described intellectual privacy as consisting of four elements: "the

---

213. *Kovacs*, 336 U.S. at 97 (Frankfurter, J., concurring).

214. Seana Valentine Shiffrin, *What Is Really Wrong with Compelled Association?*, 99 NW. U. L. REV. 839, 873 (2005).

215. *Id.* at 875.

216. *Id.* at 874.

217. *See, e.g.*, Richards, *Intellectual Privacy*, *supra* note 37, at 425 (drawing the link between intellectual privacy and cognitive processes).

218. *Id.* at 389.

219. *Id.*

220. *Id.* Richards also wrote that intellectual privacy

> nurtures the cognitive and communicative processes by which we as individuals can come to think for ourselves. It allows us to imagine, test, and develop our ideas free from the deterring gaze or interfering actions of others. Without intellectual privacy, we would be less willing to investigate ideas and hypotheses that might turn out to be wrong, controversial, or deviant. Intellectual privacy thus permits us to experiment with ideas in relative seclusion without having to disclose them before we have developed them, considered them, and decided whether to adopt them as our own.

Id. at 425.

freedom of thought and belief, spatial privacy, the freedom of intellectual exploration, and the confidentiality of communication."[221] *Freedom of thought and belief* is "the precondition for all other political and religious rights."[222] It "protects our ability to hold beliefs"[223] by safeguarding "the individual's thoughts from scrutiny or unwilling disclosure."[224] *Spatial privacy* "refers to the protection of places—physical, social, or otherwise—against intrusion or surveillance," which "allow[s] us to think freely and without interference."[225] *Freedom of intellectual exploration* protects the individual's ability to develop new ideas and discover new truths by preserving our "right to receive, read, and engage with information in private."[226] Finally, *confidentiality of communication* "protects the relationships in which information is shared, allowing candid discussion away from the prying ears of others. It allows us to share our questions and tentative conclusions with confidence that our thoughts will not be made public until we are ready."[227]

Richards's conception of intellectual privacy prioritized the protection of autonomous thought processes, including the ability to think freely and without interference, to develop new ideas and discover new truths, and to vet our thoughts with close confidants. The preservation of autonomous thought in turn requires that we protect our right to receive, read, and engage with information; limit external scrutiny of our thought processes, including the maintenance of private spaces free from outside interference; safeguard our thoughts from the threat of unwilling disclosure; and protect those confidential communications through which we test and refine our thoughts, ideas, and beliefs.[228] Thus, Richards made explicit the connection between freedom of thought (as an element of First Amendment theory) and certain forms of privacy protection.[229] He argued "that a meaningful measure of privacy is critical to the most basic operations of expression, because it gives new ideas the room they need to grow."[230] Justice Brandeis recognized this connection in his famous dissent in *Olmstead*, tying freedom of thought to core Fourth Amendment concerns.[231] "The makers of our Constitution," Brandeis wrote, "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations," free from "unjustifiable intrusion by the Government . . . [in] violation of the Fourth Amendment."[232] Richards likewise invoked familiar Fourth Amendment

221. *Id.* at 392.

222. *Id.* at 408.

223. *Id.* at 416.

224. *Id.* at 408.

225. *Id.* at 412–13.

226. *Id.* at 417.

227. *Id.* at 421.

228. *See id.* at 392–421.

229. *Id.* at 392.

230. *Id.*

231. *See* Olmstead v. United States, 277 U.S. 438, 471–85 (1928) (Brandeis, J., dissenting), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

232. *Id.* at 478.

safeguards against intrusive surveillance, with specific protections shaped by reference to the First Amendment values sought to be preserved[233]—be it promoting democratic self-governance, truth-seeking, or preserving individual autonomy and self-realization.[234]

This connection between freedom of thought and core Fourth Amendment principles can be traced to influences predating the Revolution. It was a view drawn from both the English and the colonial experiences. In England, Chief Justice Charles Pratt[235] presided over two landmark cases challenging the Crown's use of general warrants to search and seize personal papers, and in both, Pratt affirmed the status of personal papers as a unique and invaluable form of property.[236] In *Entick v. Carrington*,[237] Pratt distinguished personal papers as a man's "dearest property . . . so far from enduring a seizure, that they will hardly bear an inspection."[238] And in *Wilkes v. Wood*,[239] personal papers were described as the "promulgation of our most private concerns" and as "affairs of the most secret personal nature," the seizure of which perpetrates a harm for which almost "no reparation whatsoever could be made."[240] As one member of the House of Commons commented in parliamentary debates associated with these cases, personal papers are "often dearer to a man than his heart's blood."[241] These events were closely followed in the colonies, which "absorbed the message of the separate iniquity of seizing papers [and] carried *Entick* into American law."[242]

In *The Original Fourth Amendment*, Laura Donohue described in brilliant detail how "these judicial challenges—and the legal treatises on which they were based—were to profoundly shape the Founding Fathers' introduction and understanding of the Fourth Amendment."[243] Even before the ratification of a Federal Constitution and Bill of Rights, "the newly formed American states

233. *See, e.g.*, Richards, *Intellectual Privacy*, *supra* note 37, at 431–44 (providing four practical examples of "ways in which the collection and use of personal information about intellectual activities can threaten First Amendment values").

234. *See, e.g.*, *id.* at 407, 431–44 (arguing that "no matter which theory we proffer for why we protect speaking and writing, freedom of thought is essential to that theory").

235. *See generally Charles Pratt*, 46 DICTIONARY OF NATIONAL BIOGRAPHY 285–88 (Sidney Lee ed., 1896).

236. Entick v. Carrington (1765) 19 How. St. Tr. 1029; Wilkes v. Wood (1763) 98 Eng. Rep. 489.

237. (1765) 19 How. St. Tr. 1029.

238. *Entick*, 19 How. St. Tr. at 1066.

239. (1763) 98 Eng. Rep. 489.

240. *Wilkes*, 98 Eng. Rep. at 490.

241. *See* 16 Parl. Hist. Eng. HC (1795) 6, 10.

242. Dripps, *supra* note 3, at 83.

243. Donohue, *Original Fourth Amendment*, *supra* note 32, at 1199; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) ("The Founding generation crafted the Fourth Amendment as a 'response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.'" (quoting Riley v. California, 134 S. Ct. 2473, 2494 (2014))); *id.* at 2251 (Alito, J., dissenting) (quoting affirmatively from the same passage of *Riley*).

objected to the use of promiscuous search and seizure."[244] Utilizing fairly consistent language, early state constitutions provided express protection for papers, as distinct from other personal property (i.e., effects).[245] Likewise, during ratification of the Federal Constitution, various commentators and several state conventions proposed the addition of analogous provisions.[246] This carried through to the final, now familiar, language of the Fourth Amendment, identifying "persons, houses, papers, and effects" as related but discrete areas of concern.[247] In its earliest decisions interpreting and applying this text, the Supreme Court returned to the English cases and colonial experience, acknowledging their profound influence on the framing of the Fourth Amendment. In *Boyd v. United States*,[248] for instance, Justice Bradley wrote of *Entick* and the surrounding turmoil:

> As every American statesmen, during our revolutionary and formative period as a nation, was undoubtedly familiar with this monument of English freedom, and considered it as the true and ultimate expression of constitutional law, it may be confidently asserted that its propositions were in the minds of those who framed the Fourth Amendment to the Constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures.[249]

And it was in *Boyd* that the Court affirmed the special status of "a man's private books and papers."[250]

The *Boyd* Court recognized two constitutional grounds for this expansive, almost absolute protection.[251] The Fourth Amendment protected personal papers as a subset of personal property more generally, severely restricting governmental trespass absent a sufficient competing interest in that property beyond mere evidence of a crime.[252] Buttressing these protections were those provided by the Fifth Amendment right against self-incrimination, which shielded papers that were testimonial in nature.[253] Working in tandem—such

244. Donohue, *Original Fourth Amendment*, *supra* note 32, at 1264.

245. *Id.* at 1264–69 (discussing the various state provisions).

246. *See id.* at 1283–93 (describing efforts by various states engaged in the ratification process to guarantee protection against unreasonable search and seizure by incorporation in a Bill of Rights).

247. *See* U.S. CONST. amend. IV.

248. 116 U.S. 616 (1886), *overruled by* Warden v. Hayden, 387 U.S. 294 (1967).

249. *Boyd*, 116 U.S. at 626–27.

250. *Id.* at 623.

251. *See id.* at 633, 635 (recognizing that "the 'unreasonable searches and seizures' condemned in the Fourth Amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the Fifth Amendment," and arguing that these "constitutional provisions for the security of person and property should be liberally construed").

252. *See id.* at 633; *see also* Gouled v. United States, 255 U.S. 298, 308–11 (1921) (finding a Fourth Amendment violation where a warrant was used to seize the defendants' papers, which were later used at trial), *abrogated by Hayden*, 387 U.S. 294.

253. *See Boyd*, 116 U.S. at 633; *see also* Hale v. Henkel, 201 U.S. 43, 71 (1906) (observing that seizing private papers may not be substantially different from compelling the defendant to be a witness against himself).

that they "r[a]n almost into each other"[254]—the Fourth and Fifth Amendments thus afforded almost categorical protection against the search, seizure, and evidentiary use of personal papers by government officials.

Unfortunately, these exceptional protections for personal papers proved too fragile to survive intact. In *Warden v. Hayden*,[255] the Court eliminated the mere evidence rule[256] and with it the claim to heightened protection for papers under the Fourth Amendment.[257] And in *Andresen v. Maryland*,[258] the Court found no violation of the Fifth Amendment right against compulsory self-incrimination where the target of a search warrant was not required to prepare, produce, or authenticate the papers in question.[259] In less than ten years, the Court essentially eliminated the exceptional constitutional protections for personal papers.

After *Hayden* and *Andresen*, personal papers were no longer to be uniquely valued as constituent elements of the inner workings of the mind but as mere objects, regressing to just another form of chattel. The conveyance of documents through and to third parties might have presented a challenge to this ordinary property-based approach, but the secrecy-based rule of *Ex parte Jackson*[260] allowed the Court to avoid any inconsistency.[261] When the Court moved away from an explicitly property-based approach in *Katz*, adopting instead the expectation-of-privacy test,[262] questions regarding the special status of papers might well have reemerged. Instead the Court defaulted to familiar binaries (e.g., private versus public, secrecy versus disclosure) that again superseded questions regarding privacy protections for papers qua papers. As a matter of Fourth Amendment jurisprudence, the link between freedom of thought, the Fourth Amendment, and the enumeration of "papers" as a distinct object of protection was effectively obscured.

---

254. *Boyd*, 116 U.S. at 630.

255. 387 U.S. 294 (1967).

256. *Hayden*, 387 U.S. at 300–02, 310. Under the mere evidence rule, a search warrant authorized law enforcement to search and seize "the instrumentalities of the crime (such as a murder weapon) or the fruits of the crime (such as stolen goods)" but not "items that have evidentiary value only (such as incriminating documents)." *Mere-Evidence Rule*, BLACK'S LAW DICTIONARY, *supra* note 32.

257. Although leaving the question open in *Hayden*, the Court expressly extended its rejection of the mere evidence rule to personal papers in *Fisher v. United States*, 425 U.S. 391, 409 (1976). There, the Court stated that, "[t]o the extent . . . that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment . . . the foundations for the rule have been washed away." *Fisher*, 425 U.S. at 409.

258. 427 U.S. 463 (1976).

259. *Andresen*, 427 U.S. at 472–73. In *Couch v. United States*, 409 U.S. 322 (1973), the Court held that the right against self-incrimination is personal and therefore does not apply to papers provided to a third party. *Couch*, 409 U.S. at 326–27.

260. 96 U.S. 727 (1878).

261. *Jackson*, 96 U.S. at 733.

262. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (stating that an intrusion into an individual's "constitutionally protected reasonable expectation of privacy" could "constitute a violation of the Fourth Amendment").

Current Supreme Court jurisprudence reflects both the asserted historical commitment to the protection of personal papers and the Court's failure to articulate either a consistent supporting theory or sufficient guidance as to the reach of any such safeguards. Writing for the majority in *Carpenter v. United States*,[263] Chief Justice Roberts suggested that a blanket rule permitting the warrantless search of "any personal information reduced to document form"—including "private letters"—would be untenable.[264] Yet Roberts provided no explicit rationale for excepting this particular class of papers from the traditional rule of the third-party doctrine. In that same case, several of the dissenting Justices likewise recognized that personal papers likely enjoy a special status under Fourth Amendment doctrine but conditioned that enhanced protection on an individual's property interest in those papers—characterizing their possession by a third party as a bailment.[265] Chief Justice Roberts agreed that an exception for the "modern-day equivalents" of personal papers would be "sensible" but invoked the "reasonable expectation of privacy" standard rather than the dissenters' property rationale.[266]

In the parts that follow, I propose both an animating rationale for protecting personal papers and guidelines for determining those circumstances justifying an exception to the third-party doctrine.

B. Cognitive Processes and Cognitive Artifacts

In this Part, I turn to cognitive science to demonstrate how our constitutional commitment to freedom of thought is threatened by the failure to provide adequate Fourth Amendment protections for information stored on third-party computer systems. Cognitive science refers to "the interdisciplinary study of mind and intelligence, embracing philosophy, psychology, artificial intelligence, neuroscience, linguistics, and anthropology."[267] I begin by exploring the four principal models of human cognition that have emerged within cognitive

263. 138 S. Ct. 2206 (2018).

264. *Carpenter*, 138 S. Ct. at 2222.

265. *Id.* at 2230 (Kennedy, J., dissenting) ("*Miller* and *Smith* may not apply when the Government obtains modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." (first citing *Jackson*, 96 U.S. at 733; then citing United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010))); *id.* at 2259 n.6 (Alito, J., dissenting) (declining to answer whether the warrant requirement applies to "case[s] in which someone has entrusted papers he or she owns to the safekeeping of another," and/or to cases involving a bailment); *id.* at 2269 (Gorsuch, J., dissenting) ("Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents.").

266. *Id.* at 2222 (majority opinion).

267. Paul Thagard, *Cognitive Science*, STAN. ENCYCLOPEDIA PHIL. (July 11, 2014), https://plato.stanford.edu/entries/cognitive-science/ [https://perma.cc/88X3-7TBK]; *see also* WORLD TECH. EVALUATION CTR., CONVERGENCE OF KNOWLEDGE, TECHNOLOGY, AND SOCIETY 429 (Mihail C. Roco et al., eds., 2013) (defining cognitive science as "[r]igorous research on animal and human mental functions, based on the convergence of previously separate sciences, notably cognitive psychology and neuroscience, but also including artificial intelligence and some branches of anthropology, philosophy, and education").

science, including the traditional internalist view and three variations of situated cognition theory (embodied cognition, embedded cognition, and extended/distributed cognition).[268] I then examine the role of cognitive artifacts within these models.

Cognitive artifacts are devices through and by which humans "extend cognitive abilities, such as abstract thought, memory, problem solving, and language use."[269] This baseline theory of human cognition supports the intuitive sense of the Framers that autonomous thought requires privacy of thought and that personal papers are often key to the development of ideas and beliefs. More specifically, the enumeration of "papers" as a distinct object of Fourth Amendment protection reflects an understanding (whether explicit or instinctive) that humans employ personal papers as cognitive artifacts integral to our cognitive processes. Maintaining freedom of thought therefore requires that personal papers be safeguarded against government interference. But these cognitive models do something more. They provide a conceptual structure not only to explain enhanced privacy protections for personal papers but also to justify an exception to the third-party doctrine that extends these enhanced protections to certain information stored on third-party computer systems.

Cognitive psychologist Ulric Neisser defined cognition as "all the processes by which . . . sensory input is transformed, reduced, elaborated, stored, recovered, and used."[270] But how are these intellectual processes carried out? "The central hypothesis of cognitive science is that [human cognitive processes] can best be understood in terms of [(a)] representational structures in the mind and [(b)] computational procedures that operate on those structures."[271] It is an approach that evolved from the development of modern logic and computing[272]

---

268. Paul Smart et al., *The Cognitive Ecology of the Internet*, *in* COGNITION BEYOND THE BRAIN 251, 256 (Stephen J. Cowley & Frédéric Vallée-Tourangeau eds., 2d ed. 2017) (noting the shift away from the traditional view and towards situated theories over the past twenty to thirty years).

269. Philip Brey, *Theories of Technology as Extension of Human Faculties*, *in* 19 RESEARCH IN PHILOSOPHY AND TECHNOLOGY 59, 75 (Carl Mitcham ed., 2000).

270. ULRIC NEISSER, COGNITIVE PSYCHOLOGY 4 (1967).

271. Thagard, *supra* note 267.

272. *See* W. Bechtel et al., *Cognitive Science: History*, *in* INTERNATIONAL ENCYCLOPEDIA OF THE SOCIAL AND BEHAVIORAL SCIENCES 2154, 2155 (Neil J. Smelser & Paul B. Baltes eds., 1st ed. 2001). Bechtel et al. offer the following reflection on those early influences:

> One of the central inspirations for cognitive science was the development of computational models of cognitive performance, which bring together two ideas. First, conceiving of thought as computation was an offshoot of the development of modern logic. In his 1854 book, *The Laws of Thought*, the British mathematician George Boole demonstrated that formal operations performed on sets corresponded to logical operators (and, or, not) applied to propositions; Boole proposed that these could serve as laws of thought. Second, conceiving of computers as devices for computation can be traced back to Charles Babbage's plans in the 1840s for an 'analytical engine' and his collaboration with Lady Lovelace (Ada Augusta Byron) in developing ideas for programming the device. These ideas gained new life in the 1930s and 1940s with the development of automata theory (especially the Turing machine), cybernetics (centered on Norbert Weiner's feedback loops), designs for implementing Boolean operations via electric on/off switches (Claude Shannon), and information theory (also Shannon). Implementation became possible with the invention

and continues to draw on these foundations:

> Most work in cognitive science assumes that the mind has mental representations analogous to computer data structures, and computational procedures similar to computational algorithms. Cognitive theorists have proposed that the mind contains such mental representations as logical propositions, rules, concepts, images, and analogies, and that it uses mental procedures such as deduction, search, matching, rotating, and retrieval.[273]

Utilizing these basic elements of mental representation and computational procedure, cognitive science theorizes functional models of information processing—perception, attention, language, memory, and thought.

In constructing these functional models, some of the most basic and contested questions revolve around the structure of the cognitive system in which these processes occur. Broadly speaking, two models of cognitive processing and cognitive systems have emerged. The *traditional internalist view* is of the mind as "an abstract information processor,"[274] conceptually distinct from the corporeal body,[275] with "[p]erceptual and motor systems . . . serv[ing] merely as peripheral input and output devices."[276] *Situated cognition theory,* on the other hand, shifts away from focusing on "cognitive processes realized in the brain [and] towards cognitive processes involving brain, body, and the environment."[277] This broad theory can be roughly divided into three distinct but related theses:

> First, the *embodied cognition thesis*, which claims that cognition depends on, and is sometimes constituted by, the human body. Second, the *embedded cognition thesis*, which claims that our cognitive processes are sometimes shaped but not constituted by bio-external resources. Third, the [*extended cognition thesis*], which claim[s] that cognitive states and processes, under certain conditions, are distributed across embodied agents and cognitive artifacts or other bio-external resources.[278]

As these descriptions suggest, key points of differentiation between these various theses include the locus of cognition and the role of bioexternal resources (including cognitive artifacts) in cognitive systems and processes.

> of electrical circuits, vacuum tubes, and transistors and was put on a fast track by World War II . . . .

Id.

273. Thagard, *supra* note 267.

274. Margaret Wilson, *Six Views of Embodied Cognition*, 9 PSYCHONOMIC BULL. & REV. 625, 625 (2002).

275. *See* Brey, *Human-Computer Interaction*, *supra* note 56, at 388 ("Traditionally, cognitive scientists have located information processing tasks in the head; information processing, or cognition, is thought to be done by minds, and minds alone."); Robert A. Wilson & Lucia Foglia, *Embodied Cognition*, STAN. ENCYCLOPEDIA PHIL. (Dec. 8, 2015), https://plato.stanford.edu/entries/embodied-cognition/ [https://perma.cc/D3HD-E28A].

276. Wilson, *supra* note 274, at 625.

277. Smart et al., *supra* note 268, at 256.

278. *Id.* (emphases added) (citations omitted). "Some theorists take these three approaches as a package deal, whereas others defend only one of these approaches." *Id.*

Proponents of embodied cognition claim that "aspects of the agent's body beyond the brain play a significant causal or physically constitutive role in cognitive processing,"[279] and thus "that the mind must be understood in the context of its relationship to a physical body that interacts with the world."[280] We can distinguish between the "weak" and "strong" forms of embodied cognition by reference to the nature and degree of integration between mind and body. "Weak embodied cognition claims that human cognitive processes sometimes depend on and are shaped by the body but are not constituted by it. Strong embodied cognition, on the other hand, claims that cognition is partly constituted by the body."[281] In either case, bioexternal resources play no constitutive role in human cognitive processes.[282]

Building on the distinction between the weak and strong forms of embodied cognition, it is helpful to generalize the key point of differentiation as between (a) those resources that merely aid cognition[283] and (b) those resources that are constitutive of a cognitive process or system.[284] Note that in applying this distinction to the embodied cognition thesis, the relevant resource to be considered is the physical body in its relation to the mind.[285] Embedded cognition and extended cognition move beyond the mind-body conception to consider whether artifacts and other external resources merely aid our cognitive processes or may function as constitutive elements of certain cognitive processes residing in a cognitive system.[286] Embedded cognition generally treats these external resources as aids to cognition (e.g., scaffolding).[287] Extended cognition, on the other hand, recognizes that external resources may be "potentially integrated deeply into the cognitive processes of their users, thereby extending their cognitive processes" as constitutive elements of that system.[288] Although there is significant variation in the precise contours of this approach, at the approach's fullest is "the claim that new layers of non-biological scaffolding (pens, papers, software packages and the like) might literally become incorporated into the very mechanisms of (some kinds of) human thought."[289]

In considering the role of external resources within these processes and systems, we pay particular attention to cognitive artifacts. An *artifact* is generally defined as "a physical object intentionally designed, made, and used for a particular purpose."[290] *Cognitive artifacts*, generally speaking, are a specific type

279. Wilson & Foglia, *supra* note 275.

280. Wilson, *supra* note 274, at 625.

281. Smart et al., *supra* note 268, at 257.

282. *See id.*

283. *Id.* at 259–60.

284. *Id.*

285. *Id.* at 263.

286. *Id.* at 259–60, 269–70.

287. *Id.* at 259–60.

288. *See id.* at 259.

289. Collins, Clark & Shrager, *supra* note 55, at 361 (Clark's "The Blind Carpenter: A Reply to Harry Collins").

290. Richard Heersmink, *A Taxonomy of Cognitive Artifacts: Function, Information, and*

of artifact, the purpose of which is to aid, enhance, or improve cognition.[291] Philosophy and technology scholar Robert Clowes offered this definition:

> Provisionally and pragmatically . . . we shall define cognitive artefacts as artificial devices which either perform functions that, were they carried out in the brain should count as cognitive, or significantly support, extend or complement such functions . . . . At this stage, we need not defend a strong position on whether cognitive technologies can become actual parts of our minds, and thus extend our minds, as the thesis of the extended mind contends, or merely act as a new sort of environment, niche or scaffold in which our minds operate. We merely hold that we, and our minds, have undergone profound changes, as we create and adopt new cognitive technologies.[292]

Psychologist Donald Norman, who is widely credited with introducing the concept, defined cognitive artifacts as "artificial devices that maintain, display, or operate upon information in order to serve a representational function and that affect human cognitive performance."[293] Expanding on the functional aspect, Philip Brey identified the ability of a cognitive artifact "to represent, store, retrieve and manipulate information,"[294] while Nancy J. Nersessian emphasized "the cognitive properties of generating, manipulating, or propagating representations."[295] As Richard Heersmink observed, these definitions have three elements in common: "cognitive artifacts are defined as (a) human-made, physical objects" that (b) "provide (and sometimes manipulate or process) representational information," and (c) "are deployed by human agents for the purpose of functionally contributing to performing a cognitive task."[296] According to Heersmink, it is the last of these elements that is the "most distinctive property" of a cognitive artifact.[297] Brey echoed this point, remarking that a "distinguishing feature of cognitive artifacts is that they do not just

---

Categories, 4 REV. PHIL. PSYCHOL. 465, 468 (2013) [hereinafter Heersmink, *Taxonomy*]; *see also* Beth Preston, *Artifact*, STAN. ENCYCLOPEDIA PHIL. (July 18, 2018), https://plato.stanford.edu/entries/artifact/ [https://perma.cc/85DF-HWWM] ("[A]rtifacts are objects made intentionally, in order to accomplish some purpose.").

291. Heersmink, *Taxonomy*, *supra* note 290, at 467–68 (discussing EDWIN HUTCHINS, COGNITION IN THE WILD 172 (1995)).

292. Robert Clowes, *Thinking in the Cloud: The Cognitive Incorporation of Cloud-Based Technology*, 28 PHIL. & TECH. 261, 264 (2015) (citations omitted).

293. Norman, *supra* note 58, at 17. Common examples include "a string tied around the finger as a reminder, a calendar, a shopping list, and a computer." Hutchins, *Cognitive Artifacts*, *supra* note 57, at 126.

294. Brey, *Human-Computer Interaction*, *supra* note 56, at 385.

295. Nancy J. Nersessian, *Interpreting Scientific and Engineering Practices: Integrating the Cognitive, Social, and Cultural Dimensions*, *in* SCIENTIFIC AND TECHNOLOGICAL THINKING 17, 42 (Michael E. Gorman et al. eds., 2005).

296. Heersmink, *Taxonomy*, *supra* note 290, at 471. Although Heersmink defined cognitive artifacts as physical objects, Norman allowed that "cognitive artifacts . . . [may] include mental as well as material elements." Hutchins, *Cognitive Artifacts*, *supra* note 57, at 126 (citing DONALD A. NORMAN, THE PSYCHOLOGY OF EVERYDAY THINGS (1987)) ("Rules of thumb, proverbs, mnemonics, and memorized procedures are clearly artifactual and play a similar role to objects in some cognitive processes.").

297. Heersmink, *Taxonomy*, *supra* note 290, at 471.

function as objects of cognition, like other structure [sic] in the world, but that they become integral components of the information processing task itself."[298]

Focusing on these last two points, there is a certain amount of disagreement inherent in the various models of human cognition regarding both the precise manner in which cognitive artifacts contribute to the performance of a cognitive task and the degree to which cognitive artifacts are integrated into the cognitive process itself. For purposes of this Article, a few examples will suffice. Edwin Hutchins posited that "[c]ognitive artifacts are involved in a process of organizing functional skills into *functional systems*" and thereby "produce cognitive effects by bringing functional skills into coordination with various kinds of structure."[299] Heersmink argued:

> The informational properties and functionalities of [cognitive] artefacts are crucial for performing a wide range of cognitive tasks, including navigating, calculating, planning, remembering, decision-making, and reasoning . . . . The function of cognitive artefacts . . . is to provide task-relevant information, thereby *complementing* internal storage and processing systems and making certain cognitive tasks easier, faster, more reliable, or possible at all. A map, for example, is a cognitive artefact because its function is to provide task-relevant information used for navigating.[300]

Thus, "cognitive function [may be characterized] as an emergent property of the interaction between intentional, embodied agents, and cognitive artefacts."[301]

In an effort to more clearly illustrate the relationship between cognitive artifacts and the cognitive tasks for which they are employed, I will closely examine one such task: memory. Most people are all too aware of our increasing reliance on digital devices and internet access.[302] Most apparently, this interdependence evidences our desire for connecting—linking together individuals and organizations, whether synchronously or asynchronously, at virtually any time and from any place. But it also reflects our growing appetite for access to information—both the information that we ourselves create and information available from other known and unknown sources. Our ubiquitous smartphones are themselves a powerful example, with processing speeds and self-contained data storage capabilities[303] that were almost unimaginable just years earlier. A variety of native applications—software residing on and running

298. Brey, *Human-Computer Interaction*, *supra* note 56, at 388.

299. Hutchins, *Cognitive Artifacts*, *supra* note 57, at 127.

300. Richard Heersmink, *The Metaphysics of Cognitive Artefacts*, 19 PHIL. EXPLORATIONS 78, 78–79 (2016) [hereinafter Heersmink, *Metaphysics*] (citations omitted).

301. *Id.* at 85. So, for instance, if the representation structure of a cognitive artifact contains information that is task relevant, this information is perceived and then processed by internal systems. *See id*. at 78–85.

302. *See* Betsy Sparrow et al., *Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips*, 333 SCIENCE 776–78 (2011) (presenting a study on the effects of digital devices and the internet).

303. For example, in 2014 the 4.9-ounce iPhone 4S offered up to 64 GB of capacity, with both cellular and wireless capabilities. *iPhone 4S—Technical Specifications*, APPLE.COM (Aug. 15, 2014), https://support.apple.com/kb/sp643?locale=en_US [https://perma.cc/EM3T-FQPN].

in the smartphone environment—allow the user to easily create, modify, organize, and access this locally stored data.[304] Other applications perform these and other data functions without the involvement and/or knowledge of the user.[305] Of course, these same devices also provide network access through web browsers (e.g., Safari or Chrome), email clients (e.g., Outlook or Apple's Mail), and remote storage applications (e.g., Dropbox or Google Drive). Through the network, users gain access to an almost inconceivable amount of remotely stored data, as well as network-based applications providing data creation, modification, organization, and access functions similar to those provided by native applications.

One phenomenon of this environment—where the amount of available data is so great, and where that data is easily created, stored, organized, and accessed—is what has been called *memory offloading*.[306] "Inundated by more information than we can possibly hold in our heads, we're increasingly handing off the job of remembering" to our devices and network-based applications.[307] This offloaded memory usually takes two forms. The first form can be broadly thought of as generalized information about our individual lives. Rather than remembering phone numbers and addresses, we store them in our contacts database. Events are calendared electronically and forgotten until the reminder pops up on our phone. Facts contained in correspondence are stored in searchable email archives. Meeting notes are drafted and stored on a remote access server. The second form is generalized information about the world at large. What is the capital of Panama? What is the difference between spiders and insects? What is the square root of 196? Who wrote the poem "Ode to Autumn"? Rather than committing these facts to memory, we turn to Google. And, having looked them up once, "[w]e don't even have to remember the answers—we can just look them up again."[308]

This phenomenon has been described as a process in which "[w]e are becoming symbiotic with our computer tools."[309] Or, in the words of

304. *See Hybrid vs Native Mobile Apps—The Answer Is Clear*, Y MEDIA LABS, https://ymedialabs.com/hybrid-vs-native-mobile-apps-the-answer-is-clear [https://perma.cc/V7CA-3GXY] (last visited Oct. 18, 2018) ("[N]ative applications have the significant advantage of being able to easily access and utilize the built-in capabilities of the user's device . . . .").

305. *See, e.g.*, Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED (Apr. 14, 2018, 7:00 AM), https://www.wired.com/story/app-permissions/ [https://perma.cc/2EL3-5JWD]; *see also* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Cell phone users often may not know whether particular information is stored on the device or in the cloud . . . .").

306. John F. Nestojko et al., *Extending Cognition to External Agents*, 24 PSYCHOL. INQUIRY 321, 321 (2013) ("Humans have tried to offload memory tasks for as long as we have recorded history . . . . The issue is how the Internet has accelerated and changed the process.").

307. Annie Murphy Paul, *Your Head Is in the Cloud*, TIME (Mar. 12, 2012), http://content.time.com/time/subscriber/article/0,33009,2108040-1,00.html [https://perma.cc/Q23A-GE75].

308. Ed Yong, *The Extended Mind—How Google Affects Our Memories*, DISCOVER: NOT EXACTLY ROCKET SCIENCE (July 14, 2011, 2:00 PM), http://blogs.discovermagazine.com/notrocketscience/2011/07/14/the-extended-mind-how-google-affects-our-memories/#.W56q9ZNKhTY [https://perma.cc/9SQ6-AVAC].

309. Paul, *supra* note 307; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)

anthropologist Amber Case, "We are all cyborgs now."[310] The metaphor is, in many respects, rather appropriate. Drawing on a definition from 1960s space exploration, Case defined a cyborg as "an organism to which exogenous components have been added for the purpose of adapting to new environments."[311] In this case, that new environment is one in which the amount of information both readily available to and thrust upon the individual is beyond the capacity of our organic brains.[312] We therefore outsource certain memory tasks to "exogenous components" such as smartphones, through which we create, modify, organize, and access information distributed across vast remote networks.[313] It is a deepening symbiotic relationship between users and computers that appears to be evolving toward an interconnected system—a system in which we "remember less by knowing information than by knowing where the information can be found."[314] As we offload memory to digital devices and networks, "forgetting" the substantive information, we are getting better at remembering where the information is and/or how to find it.[315]

A simple example reframes the process of memory offloading to illustrate how cognitive artifacts are deployed in the new information environment. As described previously, Dropbox is a remote file-storage application that automatically syncs copies of a user's digital files to Dropbox's servers.[316] These files are then accessible to the user across multiple devices.[317] In the context of several of the cognitive models previously described, these stored files function as classic examples of cognitive artifacts, in that they are artificial devices (here, intangible) that carry representational information (little different from a shopping list, calendar, or diary) created and deployed "for the purpose of functionally contributing to performing a cognitive task"[318] such as memory or problem solving.

This conception of personal papers and their digital equivalents as cognitive artifacts is entirely consistent with historical protections for personal papers:

> The particular concern of eighteenth-century commentators focused

("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (quoting Riley v. California, 134 S. Ct. 2473, 2484 (2014))).

310. Amber Case, We Are All Cyborgs Now, Speech at TEDWomen 2010, (Dec. 2010), https://www.ted.com/talks/amber_case_we_are_all_cyborgs_now [https://perma.cc/GE46-AV9J].

311. *Id.* at 0:30.

312. *See* Richard Heersmink, *Dimensions of Integration in Embedded and Extended Cognitive Systems*, 14 PHENOMENOLOGY & COGNITIVE SCI. 577, 581 (2015) [hereinafter Heersmink, *Dimensions of Integration*].

313. Carina Chocano, *The Dilemma of Being a Cyborg*, N.Y. TIMES MAG. (Jan. 27, 2012), https://www.nytimes.com/2012/01/29/magazine/what-happens-when-data-disappears.html [https://perma.cc/6FQW-MZT5] ("We've outsourced our memories to external devices. The result is that we no longer trust our memories.").

314. Sparrow et al., *supra* note 302, at 778.

315. *Id.*

316. *See* Shallman, *supra* note 154, at 50.

317. *Id.*

318. Heersmink, *Taxonomy*, *supra* note 290, at 471.

> on papers, such as diaries, intended solely for the use and perusal of the author. In that era, writing out one's ideas for purely private analysis and reflection was seen as an essential part of the thought process. Commentators regarded these writings as essentially unspoken thoughts that had never left the bosom of the thinker. Exposing to government scrutiny documents essential to the private development of ideas would stultify normal intellectual life and development.[319]

It was this view of personal papers as "an essential part of the thought process"[320] that justified their special status as a man's "dearest property."[321] Likewise, what distinguishes cognitive artifacts from other objects of cognition is their function as "integral components of the information processing task itself."[322]

Moreover, by offloading these files to Dropbox, the user employs additional cognitive artifacts. Using Heersmink's approach, both the Dropbox service on which the file is stored and the computer through which the file is accessed can be described as "provid[ing] task-relevant information, thereby *complementing* internal storage and processing systems and making certain cognitive tasks easier, faster, more reliable, or possible at all."[323] The concept of computer systems as cognitive artifacts is certainly more contentious. But putting aside the theoretical disputes within cognitive science, many if not most users perceive Dropbox as significantly supporting, extending, and complementing cognitive functions[324] by extending their ability to "represent, store, retrieve and manipulate information."[325] At first blush, this likely seems far afield of any historical protections for personal papers, but this is not necessarily so. The purpose of a journal or diary, for instance, is to collect and store individual representational artifacts created by the author as an integral component of personal memory, to be accessed as needed to contribute to the cognitive task of remembering.[326] Similarly, a personal library may function as a collection of potential cognitive artifacts[327] to be employed in various cognitive tasks, such as abstract thought and problem solving. Both diaries and personal libraries are paradigmatic examples in the history of constitutional protections for personal

---

319. Schnapper, *supra* note 36, at 926 (footnote omitted).

320. *Id.*

321. *Id.* at 882 (quoting Entick v. Carrington (1765) 19 How. St. Tr. 1029, 1066).

322. Brey, *Human-Computer Interaction*, *supra* note 56, at 388.

323. Heersmink, *Metaphysics*, *supra* note 300, at 79 (citations omitted).

324. Clowes, *supra* note 292, at 264.

325. Brey, *Human-Computer Interaction*, *supra* note 56, at 385.

326. *See* Heersmink, *Dimensions of Integration*, *supra* note 312, at 584; Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 380 (2011) ("When an individual records her sense impressions or draws sketches in her diary, she constructs the scaffolding of her future thoughts much as interior memories construct the scaffolding of cognition.").

327. *See* Itiel E. Dror & Stevan Harnad, *Offloading Cognition onto Cognitive Technology*, *in* COGNITION DISTRIBUTED 1, 18 (Itiel E. Dror & Stevan Harnad eds., 2008).

papers.[328]

If we accept that, at the very least, the files we upload to Dropbox may be deployed as cognitive artifacts that functionally contribute to the performance of cognitive tasks, what does this add to our understanding of Fourth Amendment protections for papers? As previously discussed, true freedom of thought requires substantial protections for privacy of thought.[329] And just as this commitment protects the inner workings of the mind, so too must it also ensure privacy for all aspects of our cognitive processes. Thus, when papers and their digital equivalents are employed as cognitive artifacts—either as aids to our cognitive processes or as aspects so integral to those processes as to be constitutive of our cognitive systems[330]—they must be protected from unreasonable government interference. The failure to do so frustrates autonomous thought, and with it our ability to freely develop new ideas, discover new truths, and test our beliefs. Yet that is the state of Fourth Amendment law when the third-party doctrine is applied in the new information environment.

C. Modifications to the Third-Party Doctrine

In this Part, I propose modifications intended to address the chilling effect that "blunt application of the third-party doctrine"[331] inflicts on autonomous thought. My proposal proceeds from the following six assumptions, drawn from the previous discussion:

1. Freedom of thought is an essential constitutional value grounded primarily but not exclusively in First Amendment doctrine.

2. Freedom of thought requires privacy of thought, with protections sufficient to safeguard freedom of thought from unreasonable government interference.

3. The enumeration of "papers" as a distinct object of Fourth Amendment protection reflects both the Founders' commitment to freedom of thought and their appreciation for the important role of personal papers in the development of thoughts, ideas, and beliefs.

4. Modern cognitive science supports the Founders' intuition as to the importance of papers to our cognitive processes.

5. Consistent with several models of cognition, papers may function as cognitive artifacts deployed by humans for the purpose of functionally contributing to a cognitive task.

6. Privacy of thought (as a necessary condition of freedom of thought) requires that papers functioning as cognitive artifacts be protected from

328. *See* Boyd v. United States, 116 U.S. 616, 624 (1886) (referencing protections for "private books and papers"), *abrogated by* Warden v. Hayden, 387 U.S. 294 (1967); Donohue, *Digital World*, *supra* note 1, at 573 (citing William T. Rintala, *The Mere Evidence Rule: Limitations on Seizure Under the Fourth Amendment*, 54 CAL. L. REV 2099, 2115–16 (1966)).

329. See *supra* Part III.A for a discussion of the necessity of substantial protections for privacy of thought.

330. Smart et al., *supra* note 268, at 259–60.

331. United States v. Davis, 785 F.3d 498, 535 (11th Cir. 2015) (Martin, J., dissenting).

unreasonable government interference.

One conclusion to draw from these assumptions is that all papers have the potential to function as cognitive artifacts; therefore, all papers should be categorically excluded from governmental search and seizure. But this would merely return us to the absolutist rule of *Boyd*, which in retrospect seems untenable given the glut of digital papers now stored on third-party servers. We might alternatively conclude that all papers should be subject to search and seizure only with a valid warrant, perhaps subject to one or more of the existing exceptions but not to the third-party doctrine. Although certainly a defensible position, this undifferentiated approach would seem to prioritize cognitive concepts (i.e., papers as cognitive artifacts) without adequate reference to the basic constitutional principles those cognitive concepts help to explain.

My conclusion is a bit more measured. These cognitive concepts provide a useful frame for understanding and appreciating the special status afforded personal papers, distinct from other forms of property, under English and early American law—an appreciation that now seems lost. That is not to say that we are compelled, in service of freedom and privacy of thought, to exempt all cognitive artifacts from governmental search and seizure. But it does suggest that additional protections, guided by historical rationales and illuminated by modern cognitive science, may be appropriate.

In fashioning a limited exemption, I attempt to avoid some of the extreme results inherent in prior proposals by neither advocating for a return to near-absolute protection nor ignoring the special status of papers and the challenges of the new information environment.[332] At the same time, however, I am mindful that the Fourth Amendment often operates best where clear boundaries both reflect and guide societal expectations.[333] It would be entirely unhelpful, for instance, given the mountains of data maintained on cloud-based services, to suggest that privacy protections might turn on a case-by-case assessment of the content of a particular paper and its role in an individual's cognitive processes.

---

332. *See, e.g.*, Price, *supra* note 106, at 249 ("'[P]apers' should be read to protect expressive and associational data, regardless of its form, how it is created, or where it is located."); Schnapper, *supra* note 36, at 874 ("[T]he Supreme Court's original view of the history and meaning of the fourth amendment was correct: seizures of papers were condemned in eighteenth-century England without respect to the validity of any underlying warrant . . . ."); Strandburg, *supra* note 25, at 622 ("[T]wo core Fourth Amendment protected areas, the home and the office[,] . . . [should] be extended to encompass certain digital social contexts."); Tokson, *Automation*, *supra* note 12, at 647 (arguing that "information disclosed only to automated systems" should be considered "private").

333. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 861–62 (2004) (positing "rule clarity" as a goal of Fourth Amendment jurisprudence); Kerr, *Third-Party Doctrine*, *supra* note 21, at 581 ("The on/off switch of the suppression remedy demands clear Fourth Amendment rules on what police conduct triggers Fourth Amendment protection and what police conduct does not."); Wayne R. LaFave, *The Fourth Amendment in an Imperfect World: On Drawing "Bright Lines" and "Good Faith"*, 43 U. PITT. L. REV. 307, 325–26 (1982) (setting forth various factors to consider when determining whether to adopt bright-line rules in the Fourth Amendment context); Melanie D. Wilson, *The Return of Reasonableness: Saving the Fourth Amendment from the Supreme Court*, 59 CASE W. RES. L. REV. 1, 39 (2008) (arguing in favor of "clear rules" in Fourth Amendment jurisprudence).

Indeed, the content of a particular paper is nearly irrelevant to its potential to function as a cognitive artifact. Instead, I will attempt to identify a series of proxies by which to distinguish a relatively narrow class of digital papers, the protection of which is most likely to serve our commitment to freedom of thought without unduly burdening society's interest in effective law enforcement.

The Supreme Court's 2018 decision in *Carpenter* supports this more nuanced approach.[334] Recognizing that "seismic shifts in digital technology"[335] have transformed the traditional third-party doctrine into a blunt instrument,[336] *Carpenter* held that sharing information with a third party may *reduce* one's expectation of privacy but does not necessarily eliminate it.[337] Among the factors the Court considered in this more contextual analysis were various features of the underlying technology,[338] the scope of the surveillance enabled by that technology,[339] and the nature of the information sought by the government.[340] As to these first two factors, cloud-computing and communications systems are characterized by both the automated, pervasive collection of information and the immense capacity to store that information indefinitely—the very characteristics that the *Carpenter* Court found to caution against the uncritical extension of *Miller* and *Smith* to new technologies.[341]

The third factor—the nature of the information sought by the government—is the most relevant to my proposal. Having concluded that different categories of information may be treated differently under the third-party doctrine,[342] the Court recognized "a world of difference between the limited types of personal information addressed in *Smith* and *Miller*" (i.e., bank records and telephone numbers)[343] "and the exhaustive chronicle of location information" collected in *Carpenter*.[344] Thus, where the information sought by the government has the potential to be "sensitive"[345] and "revealing" in its

334. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221–23 (2018) (holding that individuals maintain a legitimate expectation of privacy in the extended record of their physical movements, as revealed by cell site location information, and thus that a warrant is required to obtain that information).

335. *Id.* at 2219.

336. *See id.* at 2222 (cautioning that existing Fourth Amendment jurisprudence should not be uncritically extended to new technologies).

337. *Id.* at 2221 (holding that an individual has a *reduced* expectation of privacy in shared information, rather than *no* expectation of privacy).

338. *See id.* at 2214, 2219.

339. *See id.* at 2216–18.

340. *See id.*

341. *See id.* at 2214, 2216–18.

342. *Id.* at 2216–17.

343. *See* Smith v. Maryland, 442 U.S. 735, 736–38 (1979) (telephone numbers); United States v. Miller, 425 U.S. 435, 436–38 (1976) (bank records).

344. *Carpenter*, 138 S. Ct. at 2219. The Court also held that *Smith* and *Miller* were distinguishable from *Carpenter* based on the category of information sought by the government. *See id.* at 2216–17.

345. *Id.* at 2214.

"depth, breadth, and comprehensive reach,"[346] the mere fact that it is revealed to or gathered by an automated third-party system "does not make [that information] any less deserving of Fourth Amendment protection."[347] This approach would seem to except from the third-party doctrine those cloud-computing and communication systems that collect and store personal papers containing our most personal thoughts and private concerns.

At the same time, focusing on personal papers answers one of the primary concerns of the *Carpenter* dissenters, who criticized the majority for "transform[ing] *Miller* and *Smith* into an unprincipled and unworkable doctrine."[348] The dissenters took issue, in part, with the majority's failure to "explain what makes something a distinct category of information" deserving of greater protection.[349] But personal papers offer a rare point of general, if not entirely clear or unanimous, agreement. Justice Roberts's five-vote majority opinion in *Carpenter* indicated that the warrant requirement should apply to an individual's digital papers, even when those papers are held by a third party.[350] Dissents by Justices Kennedy, Thomas, and Alito argued that Fourth Amendment protections should be tethered to the text, acknowledging constitutional safeguards for an individual's "papers."[351] Justice Kennedy went a step further, acknowledging that "*Miller* and *Smith* may not apply when 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."[352] Justice Gorsuch not only accepted these propositions, but added that complete ownership of the relevant papers may not be required to assert a Fourth Amendment interest.[353]

In the following parts, I describe a subclass of personal papers that, as "a distinct category of information,"[354] are worthy of enhanced Fourth Amendment protection. As I previously argued, personal papers may serve as cognitive artifacts, functioning as key components of human cognition. Our constitutional commitment to freedom of thought requires privacy of thought and thus privacy protections for personal papers that serve this cognitive function. Such extraordinary protection is consistent with the intuition of prior generations, who wrote their intention to protect personal papers into the text of the Fourth Amendment. The following groupings—undisclosed papers, shared confidences, and directed transmissions—serve as proxies for identifying a relatively narrow band of personal papers that are most likely to serve our commitment to freedom of thought without unduly burdening society's interest in effective law

346. *Id.* at 2223.

347. *Id.*

348. *Id.* at 2230 (Kennedy, J., dissenting).

349. *Id.* at 2234.

350. *Id.* at 2222 (majority opinion).

351. *Id.* at 2227 (Kennedy, J., dissenting); *id.* at 2239 (Thomas, J., dissenting); *id.* at 2247 (Alito, J., dissenting).

352. *Id.* at 2230 (Kennedy, J., dissenting).

353. *Id.* at 2269 (Gorsuch, J., dissenting).

354. *Id.* at 2219 (majority opinion).

enforcement.

1. Undisclosed Papers

A strong claim for an exemption from the third-party doctrine can be made for papers held in personal storage that are not intended and are unlikely to be directly observed by another party. In *Smith*, the Supreme Court relied on what Matthew Tokson called the "automation rationale" to find that telephone numbers dialed by the defendant had been publicly exposed, even where the telephone company's system was entirely automated.[355] In reaching this conclusion, Tokson posited, the Court determined that "there is no legally relevant difference between disclosure of one's personal information to a third party's automated systems and disclosure to a human being."[356] Like Tokson,[357] I reject the automation rationale in large part because it perpetuates an all-or-nothing approach to privacy that, in modern application, undermines basic principles and expectations.[358] "Virtually every kind of personal online data is stored and processed by third-party automated equipment in order to route communications, detect spam and viruses, block computer hackers, or generate advertising revenue."[359] In this environment, the automation rationale "threatens to undermine privacy rights in Internet data and potentially in all new communications technologies, present and future."[360] Indeed, the *Carpenter* Court went so far as to suggest that automated information collection cuts in favor of Fourth Amendment protections, rather than against, because it creates a constant, inescapable stream of data.[361]

Tokson's insight provides one useful proxy by which to identify a workable subclass of digital papers to be exempted from application of the third-party doctrine. At the core of the historical connection between the Fourth Amendment and freedom of thought is the protection for those "papers, such as diaries, intended solely for the use and perusal of the author."[362] As the Father of Candor wrote about the *Wilkes* affair, "Any man is at liberty to think, and to put what thoughts he pleases upon paper, provided he does not publish them."[363] Another influential series of pamphlets circulated following *Wilkes* described

355. *See* Tokson, *Automation*, *supra* note 12, at 600; *see also* Smith v. Maryland, 442 U.S. 735, 744–45 (1979) (holding that no "different constitutional result is required because the telephone company has decided to automate").

356. Tokson, *Automation*, *supra* note 12, at 600; *see also Smith*, 442 U.S. at 744–45 (rejecting the petitioner's argument that automated switching equipment differs from a live operator in any constitutionally relevant respect).

357. *See* Tokson, *Automation*, *supra* note 12, at 586 (proposing that the mere disclosure of data to automated systems should not trigger the third-party doctrine where there is "only a minimal risk of eventual exposure . . . to humans").

358. *See id.* at 617–18.

359. *Id.* at 602.

360. *Id.* at 586.

361. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220, 2223.

362. Schnapper, *supra* note 36, at 926.

363. CANDOR, A LETTER FROM CANDOR, TO THE PUBLIC ADVERTISER 30 (2d ed. 1764).

personal papers as "our closest confidents."[364] For "personal papers often contain an individual's most private thoughts, never intended to be disclosed to anyone else, 'things that the world never saw and no man has a right to look upon.'"[365]

As this history makes clear, a more circumscribed reading of the special status of personal papers would emphasize the intent of the individual to keep his thoughts private—"solely for the use and perusal of the author"[366]—and thus free from government interference. In an automated system where access by a human is exceedingly unlikely,[367] at least in the absence of a government order or request, the user's intent to keep secret his thoughts from the service provider seems both clear and reasonable. In this context, rigid application of the third-party doctrine and the automation rationale, without regard for the user's intent to disclose, fails to adequately account for even a narrow conception of the role that personal papers play in the processes of human thought. Whether personal papers are understood as "the private workings of a person's mind"[368] or as cognitive artifacts "deployed by human agents for the purpose of functionally contributing to performing a cognitive task,"[369] the basic values of freedom and privacy of thought require at the very least that undisclosed papers remain protected from government interference.

Applying these principles in the cloud-computing environment, the strongest claim for exemption from the third-party doctrine would be for the personal storage of digital papers maintained by the user of a cloud-based service where those papers are not intended and are unlikely to be directly observed by another party. A remote possibility that the service itself might access the digital paper in its ordinary course of network management would be irrelevant, as the intent to maintain privacy through nondisclosure does not require perfect concealment.[370] Common applications of this exemption would include files maintained in remote storage (e.g., Dropbox, Google Drive, iCloud) and photo applications (e.g., Flickr, Photobucket), files replicated in automated back-up systems (e.g., Carbonite, iDrive), files created in cloud-based applications (e.g., Microsoft Office, Google Docs), and curated files in

364. CHARLES WYNDHAM & GEORGE MONTAGU-DUNK, A LETTER TO THE RIGHT HONOURABLE THE EARLS OF EGREMONT AND HALIFAX, HIS MAJESTY'S PRINCIPAL SECRETARIES OF STATE, ON THE SEIZURE OF PAPERS 8 (1763).

365. Schnapper, *supra* note 36, at 890 (quoting WYNDHAM & MONTAGU-DUNK, *supra* note 364, at 25).

366. *Id.* at 926.

367. Tokson, *Automation*, *supra* note 12, at 607 (noting that even the least intrusive opportunities for human observation have nearly disappeared as "network monitoring and threat-response processes have themselves increasingly become automated").

368. Dripps, *supra* note 3, at 66–67 (summarizing the views of Chief Justice Pratt in *Entick v. Carrington*).

369. Heersmink, *Taxonomy*, *supra* note 290, at 471.

370. *See, e.g.*, CANDOR, *supra* note 363, at 30 (noting that protections for private papers rest on the intent to remain unpublished, rather than some form of perfect concealment); *see also* Carpenter v. United States, 138 S.Ct. 2206, 2216–17 (2018) (concluding that the third-party doctrine does not necessarily apply to information created by the service provider in the ordinary course of business).

organization and annotation applications (e.g., Evernote, Scrivener). This exemption would also apply to unsent drafts of emails and other forms of communication.

2. Shared Confidences

A somewhat more nuanced claim for an exemption from the third-party doctrine can be made for papers shared within certain discrete groups of individuals. Neil Richards has observed that "the development of ideas and beliefs" occurs not only in "solitary contemplation" but often in "collaboration with a few trusted confidants."[371] Indeed, both *Entick* and *Wilkes*, the leading English cases on protections for personal papers, involved the collaboration of like-minded provocateurs.[372] Helen Nissenbaum embraced a similar notion,[373] recognizing that "[i]n some contexts, people expect shared information to be held in strict confidence or limited to a small group of confidants."[374] Under the third-party doctrine, however, the exposure of information among confidants may well vitiate Fourth Amendment protections.[375] But this all-or-nothing approach "means failing to recognize degrees of privacy in the Fourth Amendment context," for "it treats exposure to a limited audience as morally equivalent to exposure to the whole world."[376]

Tying this back to cognitive science, it may be helpful to introduce the *collective cognition* model—"forms of cognition in which the relevant cognitive processes (e.g., reasoning, remembering and problem-solving) are distributed across a collection of individuals"[377]—as well as the closely connected concepts of *collective memory* and *transactive memory*. Collective memory

> concerns the manner in which information is represented in a group. Information may be shared collectively among all of the individuals in a group such that each person possesses knowledge in common, or alternatively, information may be distributed or divided among individuals . . . . [Thus,] group processes may result in shared memories that are different from individual memories.[378]

---

371. Richards, *Intellectual Privacy*, *supra* note 37, at 389; *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 121–22 (2007) ("[P]olitical discourse does not just occur on soapboxes before large crowds; it also thrives in private enclaves between small groups of people.").

372. *See* Donohue, *Original Fourth Amendment*, *supra* note 32, at 1196–204.

373. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 141–42 (2004) (discussing norms of information flow in the context of friendship).

374. *See* Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 382–83 (2013) (discussing Nissenbaum, *supra* note 373).

375. *See* Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); then citing United States v. Lee, 274 U.S. 559, 563 (1927))).

376. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

377. Smart et al., *supra* note 268, at 272.

378. Mary Susan Weldon & Krystal D. Bellinger, *Collective Memory: Collaborative and*

Transactive memory may best be thought of as a group strategy for managing large amounts of information.[379] "Individuals create a division of labor for encoding, storing, and retrieving task-relevant information; each individual specializes in one or more knowledge domains . . . . [W]hen individuals need information in others' areas of expertise, they can query those experts rather than having to invest personally in learning that information."[380]

These are admittedly contentious theories presented—not for the truth of the matter but merely to illustrate how collaborative freedom of thought might be understood. As an example, one potential consequence of distributing cognitive tasks among a group of collaborative individuals is the emergence of distinct thoughts and ideas generated from "shared memories that are different from individual memories"[381]—thoughts and ideas beyond those accessible to the individual in isolation—and thus distinctly valued. From this perspective, the collaborative processes of collective cognition present unique challenges for freedom and privacy of thought. Far from intending to maintain secrecy through nondisclosure, each individual within the collective intends to share his personal papers with the group. Thus, where "the development of ideas and beliefs" occurs in "collaboration with a few trusted confidants,"[382] protection for autonomous thought might well require that we safeguard the processes by which "[i]nformation may be shared,"[383] including the sharing of personal papers.

The question, of course, is where do we draw the line between protecting "collaboration with a few trusted confidants"[384] and evisceration of the third-party doctrine? I suggest two key factors: First, the use of access controls. And second, limitations on the number and nature of individuals permitted access. Restricted access is a well-developed concept in regard to privacy rights in spaces, objects, and communications. One particularly relevant line of cases

---

Individual Processes in Remembering, 23 J. EXPERIMENTAL PSYCHOL. 1160, 1161 (1997) (citations omitted). Weldon and Bellinger identified at least four conceptions of collective memory. *See id.* at 1160–61. The first is that "remembering may take place as a social activity" in which people "collaborate to recall events." *Id.* at 1160. What emerges are "different individuals' recollections," in the context of and influenced by the "social context." *Id.* The second recognizes that individual remembering "is situated within a larger culture or group which, in the practice of its activities, teaches its members to use memory in a particular way." *Id.* at 1161. This explains, in part, why "the content and process of recall differ across cultures." *Id.* The third, discussed here, "concerns the manner in which information is represented in a group." *Id.* Finally, collective memory can be socially and culturally important, because it frames our perception of various individuals, groups, and events. *Id.*

379. Erez Reuveni, *Copyright, Neuroscience, and Creativity*, 64 ALA. L. REV. 735, 766–67 (2013) (discussing transactive memory in the context of small group dynamics).

380. Y. Connie Yuan et al., *Access to Information in Connective and Communal Transactive Memory Systems*, 34 COMM. RES. 131, 132–33 (2007). Key to the success of such a system is what has been called *expertise recognition*. *Id.* at 133. Essentially, the effective retrieval of dispersed information in a traditional transactive memory system requires each member of the group to know "whom to query for information or answers in areas of expertise outside their own." *Id.*

381. Weldon & Bellinger, *supra* note 378, at 1161.

382. Richards, *Intellectual Privacy*, *supra* note 37, at 388–89.

383. Weldon & Bellinger, *supra* note 378, at 1161.

384. Richards, *Intellectual Privacy*, *supra* note 37, at 388–89.

holds that individuals have a Fourth Amendment interest in password-protected and/or encrypted digital files.[385] Applying this principle to cloud computing, the adequacy of restricted access would turn on the access controls available on a particular platform, the default settings for that platform, and affirmative steps by the user to limit access.

But how much access is too much? Apart from the binary default requirements of absolute concealment and nondisclosure, the Fourth Amendment has little to say regarding the sharing of information among small groups of individuals.[386] The First Amendment, however, may offer some guidance. In *Roberts v. United States Jaycees*,[387] the Supreme Court characterized the freedom of association as serving, in part, to foster special communities of thought[388] in which ideals and beliefs are cultivated.[389] Recognizing, however, that not all communities serve these values, the Court sought to distinguish between those communities with strong associational claims and those "lacking these qualities."[390] It identified several relevant characteristics, including size, purpose, policies, selectivity, and congeniality.[391] Relatively small, highly selective groups were to be favored, particularly where critical aspects of the relationship were secluded from others.[392] Given the instrumental connection between freedom of thought and freedom of association, these same factors may be applied to determine whether the size and nature of a particular collaborative group having shared access to cloud-based digital papers serves the constitutional values of autonomous thought.

3. Directed Transmissions

Finally, the strongest claim for an exemption from the third-party doctrine can be made for email and other forms of directed electronic communication, the status of which remains unsettled. As a subset of shared confidences, privacy protections for directed transmissions—communications directed to a particular person, generally to the exclusion of others—remain uniquely valued as a matter of law and tightly bound to their constitutional pedigree. In *Ex parte Jackson*, the Supreme Court held that "[l]etters and sealed packages . . . are as fully guarded

385. Trulock v. Freeh, 275 F.3d 391, 403–04 (4th Cir. 2001) (holding that one user of a shared computer lacked the authority to consent to the search of another user's password-protected files); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1021 (2010) ("Storing [a] file on a password-protected server is the virtual equivalent of keeping it in a home."); Michael Mestitz, *Unpacking Digital Containers: Extending* Riley*'s Reasoning to Digital Files and Subfolders*, 69 STAN. L. REV. 321, 354–55 (2017) (discussing cases in which password-protection and/or encryption were key factors).

386. *See generally* Bedi, *Facebook*, *supra* note 19 (proposing that the Fourth Amendment should, through the mosaic theory, provide a level of protection for group communication).

387. 468 U.S. 609 (1984).

388. *Roberts*, 468 U.S. at 620.

389. *Id.* at 618–19.

390. *Id.* at 620.

391. *Id.* (noting that other characteristics might also be pertinent in a particular case).

392. *Id.*

from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[393] Referencing the Fourth Amendment explicitly, the Court declared:

> The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be . . . . [T]hey can only be opened and examined under like warrant . . . as is required when papers are subjected to search in one's own household.[394]

This remains the law today, more than 140 years after it was decided.[395]

What of email and other forms of directed electronic communication, in which third-party intermediaries and online service providers process and store the information? Absent a recognized exception to the third-party doctrine, email would seem to constitute information exposed to the public (i.e., to a third-party intermediary analogous to the telephone company in *Smith*).[396] Nevertheless, it is usually presented as settled law that *Jackson* applies equally to email.[397]

> First, for government officials to access the contents of e-mails or other electronic communications, they must obtain a warrant based upon probable cause absent a warrant exception. Second, if the government seeks non-content information such as subscriber information, the to/from line on an e-mail, or the IP addresses of websites visited, a subpoena will generally suffice.[398]

Officials of the U.S. Department of Justice have publicly stated that the department accepts this content/non-content distinction.[399] But others push back on this assertion. At a recent public event, Jennifer Lynch of the Electronic Frontier Foundation reported that government litigators had in certain cases sought to "undermine . . . settled law, or what we thought was settled law" regarding Fourth Amendment protections for the content of email.[400] Fellow panelist Laura Donohue echoed this assessment.[401] It is worth noting that the Supreme Court has yet to weigh in on the matter and the lower courts are more divided on the question than many have suggested.[402]

---

393. *Ex parte* Jackson, 96 U.S. 727, 733 (1878).

394. *Id.*

395. Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting) (noting the continued adherence to *Ex parte Jackson*).

396. Smith v. Maryland, 442 U.S. 735, 737 (1979).

397. *See, e.g.*, THOMPSON II, CLOUD COMPUTING, *supra* note 151, at 2–3.

398. *Id.* at 6.

399. *See* Am. Bar Ass'n Criminal Justice Section, *Part 2: The New Frontier Surveillance Technology, Ethics, and the Law*, YOUTUBE (Mar. 17, 2017), https://www.youtube.com/watch?v=ocXYJSzI1sw [https://perma.cc/VZU2-5K2M] (statement of Nathan P. Judish, Senior Counsel, Comput. Crimes & Intellectual Prop. Section, Criminal Div., Dep't of Justice, at 15:45–16:20).

400. *See id.* (statement of Jennifer Lynch, Elec. Frontier Found., at 21:18–22:48) ("The Justice Department, for example, has never conceded that email is not subject to the third-party doctrine.").

401. *See id.* (statement of Laura K. Donohue, Dir., Georgetown Univ. Law Ctr., at 25:28–27:16).

402. *Compare, e.g.*, United States v. Ackerman, 831 F.3d 1292, 1304–05 (10th Cir. 2016)

If we accept that the principle of nondisclosure may, in certain contexts, survive sharply limited publication, then application of *Jackson* to email is consistent with both the collective cognition model and the historical rationale for safeguarding private papers.[403] Other forms of direct messaging using similar access controls (e.g., encryption, password protection) merit the same protection, even where the somewhat tortured analogy to regular mail is more difficult to maintain. These include direct messaging via such services as Twitter, Facebook, Instagram, and iMessage.

CONCLUSION

In this Article, I have endeavored to do three things. First, I have attempted to show that our constitutional commitment to freedom of thought is historically and properly connected to the enumeration of "papers" as a distinct object of Fourth Amendment protection. Second, I have sought to revive the connection between freedom of thought and personal papers by reference to modern models of human cognition, explaining how papers serve as cognitive artifacts functioning within a cognitive system and performing cognitive tasks. Third, I have proposed changes to the third-party doctrine that are intended to safeguard a relatively narrow class of digital papers, the protection of which is most likely to serve our commitment to freedom of thought.

As an ever-greater proportion of our transactions and interactions take place online, generating enormous amounts of data to be processed and stored by intermediaries and service providers, we must decide how legal doctrine built around desks, closets, and file cabinets should be adapted to always-on connectivity and cloud-computing networks. Although many have identified and sought to rectify the privacy problems created by this shift, it has proven difficult to articulate a limitation to the third-party doctrine that is both consistent with existing principles and feasible in practice.

This Article represents a new approach to that difficult problem. Historical understanding is supported with insight from contemporary cognitive science, translating the intuition of prior generations into current cognitive theory. These principles are then adapted into a set of proxy characteristics that distinguish those personal papers most likely to serve our constitutional values. The resulting approach provides a coherent and workable method for limiting the reach of the third-party doctrine and returning equilibrium to information privacy.

(discussing the unsettled nature of the issue), *with, e.g.*, People v. Thompson, 28 N.Y.S.3d 237, 252–53 (Sup. Ct. 2016) (presenting it as a settled issue).

403. *See* Schnapper, *supra* note 36, at 889–90 (arguing that "an individual's papers ordinarily include confidential communications with others"). See also *supra* Part III.C.2 for a discussion of collective cognition and *supra* Part III.A for a discussion of the historic rationale for safeguarding private papers.