Printed in U.S.A.
Vol. 107, No. 3

REVIVING THE PRIVACY PROTECTION ACT OF 1980

Elizabeth B. Uzelac

ABSTRACT—The federal privacy legislative scheme is composed of a fragmented patchwork of aging sector-specific statutes—many enacted prior to the advent of the home computer—that supplement the Fourth Amendment to regulate government access to information. The Privacy Protection Act of 1980 is one such statute, though few understand or utilize its protections. The Act prohibits law enforcement officials from searching for or seizing information from people who disseminate information to the public, such as reporters. Where it applies, the Act requires law enforcement officials to instead rely on compliance with a subpoena or the target's voluntary cooperation to gain access to information. While the Act clearly protects the press, its text reaches more broadly. Changes that have occurred in the information industry since the Act's passage underscore ambiguities in who and what it now protects. To revive its original privacy and speech protections, this Note advocates a reading of the Act to leverage its clear text to protect the privacy, speech, and business interests of information disseminators. Alternatively, compelling interest requirements for searches and ex ante procedural protections would protect similar privacy, speech, and business-continuity interests relevant to all sectors of today's information society.

AUTHOR—J.D., Northwestern University School of Law, 2013; M.S., Simmons College; B.M., Northwestern University. For their advice and encouragement, I thank Professor James Speta and Cindy Cohn. I am grateful to Tim Fry, Steve Golden, Laura Kolesar Gura, Susan Jacoby, Karin Lee, Andy Meerkins, Sarah Newman, Chris Sigmund, Jeff VanDam, Phil Wiese, and the *Northwestern University Law Review* staff for their thoughtful feedback and editorial work. All errors and omissions are my own.

INTRODUCTION

The federal privacy legislative scheme is a notoriously fragmented patchwork of aging sector-specific statutes.[1] Where privacy interests intersect with criminal law enforcement, privacy statutes supplement the Fourth Amendment to regulate government access to information. Public interest campaigns have exhorted Congress to enact comprehensive information privacy rules[2] and update key statutes such as the Electronic

[1] *See, e.g.*, Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2008 (2010) (calling federal privacy law "fragmented"). Different statutory regimes govern privacy in health information, financial data, children's information, and government information regulation. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2d ed. 2013) (summarizing privacy law governing sectors that deal categorically with government records, health information and genetic information, financial information, business data, educational records, and employment information). The various schemes do not even share common vocabulary or standards. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011) ("Given [personally identifiable information]'s importance, it is surprising that information privacy law in the United States lacks a uniform definition of the term.").

[2] *See generally* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009) (criticizing the demand for comprehensive privacy legislation instead of sector-specific laws); Patricia L. Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868 (2009) (responding to Professor Schwartz).

Communications Privacy Act.[3] In the meantime, decades-old statutes passed prior to the advent of the home computer govern information privacy and compelled disclosure.

The Privacy Protection Act of 1980[4] is an example of one such privacy statute. The Act prohibits law enforcement officials from searching for or seizing information from people who disseminate information to the public. Where it applies, the Act requires law enforcement officials to instead rely on compliance with a *subpoena duces tecum*[5] or the target's voluntary cooperation to gain access to information from reporters and others engaged in information dissemination.[6]

Congress enacted the Privacy Protection Act of 1980 as a response to an unpopular Supreme Court decision stemming from a controversial newsroom search at Stanford University.[7] As a result, the Act clearly protects the press, but its text reaches more broadly.[8] Since 1980, the pool of those potentially covered by the Act has increased dramatically as a result of changes in the information industry. As early as 1998, one Justice Department attorney acknowledged these changes.[9] He stated that Congress did not anticipate the "explosive grow[th] of the computer world," and that given the dramatic expansion of digital publishing and home computer usage, the Act might now in fact protect any person who publishes online.[10]

As that Justice Department attorney indicated, Congress did not deliberate over the Act with our modern information landscape in mind. As a result, three important aspects of the Act lack clarity: (1) what people it protects, (2) how the statutory classifications should be applied to digital content, and (3) what interests it protects. As to the first ambiguity, the Act can be construed to protect *any* individual intending to communicate to the

---

[3] *See, e.g.*, NOT WITHOUT A WARRANT, http://notwithoutawarrant.com (last visited May 25, 2013) ("The government should be required to go to a judge and get a warrant before it can read our email, access private photographs and documents we store online, or track our location using our mobile phones. Please support legislation that would update the Electronic Communications Privacy Act of 1986 (ECPA) to require warrants for this sensitive information and to require the government to report publicly on the use of its surveillance powers.").

[4] Pub. L. No. 96-440, 94 Stat. 1879 (codified as amended at 42 U.S.C. §§ 2000aa to 2000aa-12 (2006)).

[5] BLACK'S LAW DICTIONARY 1563 (9th ed. 2009) defines a *subpoena duces tecum* as "[a] subpoena ordering the witness to appear in court and to bring specified documents, records, or things."

[6] *See* § 2000aa(b)(3).

[7] *See* Zurcher v. Stanford Daily, 436 U.S. 547 (1978).

[8] *See* § 2000aa(a) ("[I]t shall be unlawful . . . to search for or seize any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce . . . .").

[9] *See* Mark Eckenwiler, *Applications of the Privacy Protection Act*, 8 SETON HALL CONST. L.J. 725, 729 (1998).

[10] *Id.*

public or some narrower subset of actors.[11] A textual reading of the Act reaches broadly, but the Act's muddled origins as a "First Amendment bill" and the realities of law enforcement searches and seizures of increasingly technology-intensive environments beg consideration of borderline cases.

As to the second ambiguity, how the statutory classifications apply to digital content is unclear in two ways. First, it is uncertain what digital materials constitute the "work product" and "documentary materials" that fall within the purview of the Act,[12] particularly outside a traditional press context. In a press context, work product connotes some contribution from a reporter, such as a draft article or personal notes reflecting mental impressions. Documentary materials signify material collected in preparation for distribution, absent something extra from the reporter's thoughts. Outside a traditional press context, such as in the realm of a blogger or a person who serves content to the public via mobile applications, the question of what material falls into each category is less clear. Nevertheless, the distinction matters: the statute offers different levels of protection to each category. Second, it is uncertain how commingled protected and unprotected digital materials should be treated. It is not clear whether the Act protects individual electronic files or the entire discs and computer servers that contain those files.[13] Where a server hosts many websites, whether the Act protects it from seizure may be the determining factor in whether a whole suite of services goes dark. One server seizure could result in many otherwise unrelated websites going offline, implicating the operational continuity of those businesses.

Finally, the third ambiguity involves what interests the Act protects. It can variously be characterized as protecting privacy, free speech, the press, or the operational continuity of those individuals and businesses who provide information services. Additionally, it could be limited to protecting the interests of just those people in possession of the materials sought by law enforcement, or it could protect others whose personal information is implicated by the nature of the materials.

This Note tracks two archetypical examples of people whose technological activity underscores the problems posed by the Act's ambiguities: bloggers and smartphone application developers (app developers). Bloggers distribute information to the public, though to some,

---

[11] *Compare* Edward Fenno, *Federal Internet Privacy Law*, S.C. LAW., Jan./Feb. 2001, at 32, 36 ("[I]t appears facially that nearly everyone posting messages on the Internet or with online services is covered by the Act."), *with* Viktor Mayer-Schönberger, *Beyond Privacy, Beyond Rights—Toward a "Systems" Theory of Information Governance*, 98 CALIF. L. REV. 1853, 1858 & n.22 (2010) (citing the Act as protecting "sector-specific information privacy rights").

[12] *See* § 2000aa.

[13] Documentary materials are defined by the text of § 2000aa-7(a) as "materials upon which information is recorded," including "electronically recorded cards, tapes, or discs," but they have also been defined somewhat atextually by courts. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 342 (6th Cir. 2001) (analyzing "materials" at the level of the file rather than the disc containing such files).

the idea of an at-home blogger does not align with traditional notions of the press that originally prompted enactment.[14] App developers also distribute information to the public by delivering pocket-sized services related to many topics, such as weather, finance, and gaming. While they do not necessarily gather source material from confidential sources as do the prototypical reporters who prompted the Act, app developers collect comparably private information about their customers' information consumption.[15] They also provide information infrastructure by which content is delivered to the public, whether via websites, smartphones, tablets, or other mechanisms of the app economy.

If an entire computer or server can be seized without notice, it could threaten the operational continuity of the blogger or app developer. That is, the seizure of a whole server could interrupt the continuous operation of the websites and business operations dependent upon it. Seizure of a server can cause outages of seemingly unrelated services, such as occurred in a recent Federal Bureau of Investigation raid that knocked offline more than 300 e-mail accounts, dozens of e-mail lists, and multiple websites—none of which were alleged to be involved in the anonymous bomb threats that prompted the raid.[16] The Act's protections could be negated altogether in these situations if these statutory ambiguities are not sufficiently resolved.

---

[14] The "press" is notoriously difficult to define, and the question has generated exhaustive literature outside the scope of this Note. *See, e.g.*, David A. Anderson, *Freedom of the Press*, 80 TEX. L. REV. 429, 435–46 (2002) (discussing the difficulties inherent in defining the press and various proposed solutions); Sonja R. West, *Awakening the Press Clause*, 58 UCLA L. REV. 1025, 1047–70 (2011) (counseling against an overbroad definition of the press and proposing several interpretations to allow the Press Clause "to attain its textual and functional potential").

[15] For instance, apps often collect information about what a person searches for and how long they view a particular page. The information enables and incentivizes providers to "create profiles about individuals, their interests and concerns, and even those of their family and friends." ACLU OF N. CAL., DIGITAL BOOKS: A NEW CHAPTER FOR READER PRIVACY 4 (2010), *available at* http://www.aclunc.org/issues/technology/asset_upload_file295_9047.pdf. Website providers collect similar information, so analysis that applies to app developers who host information services also applies to many website providers. *See, e.g.*, *Google Book Search Hearing—The Time Has Come to Protect Reader Privacy*, ACLU OF N. CAL., http://www.aclunc.org/issues/technology/blog/google_book_search_hearing-_the_time_has_come_to_protect_reader_privacy.shtml (last visited May 25, 2013).

[16] *See* Press Release, Riseup.net, Server Seizure, Apr. 2012, *available at* https://help.riseup.net/en/seizure-2012-april ("Disrupted in this seizure were academics, artists, historians, feminist groups, gay rights groups, community centers, documentation and software archives and free speech groups. The server included the mailing list 'cyber rights' (the oldest discussion list in Italy to discuss this topic), a Mexican migrant solidarity group, and other groups working to support indigenous groups and workers in Latin America, the Caribbean and Africa. In total, over 300 email accounts, between 50–80 email lists, and several other websites have been taken off the Internet by this action. None are alleged to be involved in the anonymous bomb threats."); *see also* Verne G. Kopytoff, *F.B.I. Seizes Web Servers, Knocking Sites Offline*, N.Y. TIMES BITS BLOG (June 21, 2011, 5:54 PM), http://bits.blogs.nytimes.com/2011/06/21/f-b-i-seizes-web-servers-knocking-sites-offline (detailing the FBI raid and the impact on the data center's clients); Paul G. Madison, *Server Seizer Leads to Unwanted Consequences*, DC METROPOLITAN BUS. L. ALERT (June 23, 2011), http://www.dcbusinesslawalert.

This Note offers an interpretation of the Act that remedies these uncertainties for law enforcement going forward. After introducing the circumstances that led to the passage of the Act, Part I details the requirements of its text and interpretations in subsequent case law.[17] Part II then briefly explains trends that have transformed the information industry since the passage of the Act. Against this backdrop, Part III introduces Professor Daniel Solove's theory of the First Amendment as an independent source of constitutional criminal procedure that protects expressive and associational activity from government information gathering. Using Solove's framework and the Act's text and history, Part III goes on to first propose and then critique a broad textual interpretation of the Act that resolves the three ambiguities enumerated above. With these critiques in mind, Part IV introduces alternative mechanisms to protect the interests implicated by the Act.

I. HISTORY AND PASSAGE OF THE PRIVACY PROTECTION ACT OF 1980

Congress enacted the Privacy Protection Act[18] out of concern over the intrusiveness of law enforcement searching and seizing materials in the press's possession. Initially framed as a First Amendment bill, the Act's text grew to encompass broad—and ill-defined—protections against compelled information disclosure.

A. The Legislative Response to Zurcher v. Stanford Daily

The Privacy Protection Act was Congress's response to the Supreme Court's 1978 ruling in *Zurcher v. Stanford Daily*.[19] *Zurcher* arose after *The Stanford Daily* published photographs of a violent clash between police and demonstrators. The demonstrators were protesting at the administrative offices of the Stanford University Hospital in response to the racially motivated firing of a janitor.[20] Authorities acquired a search warrant to search *The Stanford Daily* offices on the belief that the student newspaper possessed photographs of an assault on police officers that occurred during the demonstrations.[21]

---

com/local-news/server-seizer-leads-to-unwanted-consequences (discussing the negative repercussions for websites on the same server as those seized).

[17] Judicial and scholarly interpretations of the Act are few and far between. *Cf.* Eckenwiler, *supra* note 9 ("[T]here's very little . . . surprisingly little case law [interpreting the Act] considering it's a statute that's more than seventeen years old." (alteration in original)). The Act has now ticked past its thirtieth birthday without much change in the literature.

[18] Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. §§ 2000aa to 2000aa-12 (2006)).

[19] 436 U.S. 547 (1978).

[20] *See* Dwight L. Teeter, Jr. & S. Griffin Singer, *Search Warrants in Newsrooms: Some Aspects of the Impact of* Zurcher v. The Stanford Daily, 67 KY. L.J. 847, 849 (1979).

[21] *Zurcher*, 436 U.S. at 550–51.

The newspaper successfully challenged the search in the district and circuit courts on the grounds that the Fourth and Fourteenth Amendments forbade use of a warrant to search for materials in the possession of a nonsuspect without probable cause to believe that a subpoena would be impracticable.[22] Reversing the Ninth Circuit, the Supreme Court then held that the Fourth Amendment does not prevent a state from issuing a warrant just because the person to be searched is not suspected of a crime.[23] Specifically, the Court rejected the suggestion that the Fourth Amendment limits the government to using a *subpoena duces tecum* in such "third-party search" situations. The Court was not swayed by the fact that the search of a newspaper implicates the First Amendment.[24] Instead, the Court indicated that timely publication of the news and confidentiality of sources would be adequately protected by the requirements of a warrant application.[25]

The Court's decision thus failed to protect the press from the immediate intrusion of a break-down-the-door search and operational interruption caused by sudden seizure of materials. After the ruling, public outcry demanded protection against such abrupt intrusions.[26] President Carter directed the Justice Department to study the issues raised by *Zurcher* and assess the viability of a legislative solution.[27] The eventual solution took two years to enact, during which Congress first considered enacting broad protection for any nonsuspect third parties.[28] Rejecting that broad approach, Congress instead settled on protecting just those people engaged in public communication.[29]

---

[22] *See* Stanford Daily v. Zurcher, 353 F. Supp. 124 (N.D. Cal. 1972) (citing the Fourth Amendment to rule the search of a nonsuspect unconstitutional without probable cause to believe a *subpoena duces tecum* would be impractical), *aff'd*, 550 F.2d 464 (9th Cir. 1977), *rev'd*, 436 U.S. 547.

[23] *Zurcher*, 436 U.S. at 547, 554, 559.

[24] *Id.* at 565–66.

[25] *Id.* at 566.

[26] For a summary of the responses of major American newspapers, including responses from the *Washington Post*, *Boston Globe*, *New York Times*, and *Wall Street Journal*, see Teeter & Singer, *supra* note 20, at 854–57.

[27] *See Privacy Protection Act: Hearing on S. 115, S. 1790, and S. 1816 Before the S. Comm. on the Judiciary*, 96th Cong. 50 (1980) [hereinafter *Privacy Protection Act Hearing*] (prepared statement of Philip B. Heymann, Assistant Att'y Gen. of the United States).

[28] *See* Susan K. Erburu, Note, Zurcher v. Stanford Daily*: The Legislative Debate*, 17 HARV. J. ON LEGIS. 152, 165–73 (1980) (contrasting "press-only" and "third-party" bills considered by the Ninety-sixth Congress); *see also Privacy Protection Act Hearing*, *supra* note 27, at 59 (prepared statement of Philip B. Heymann, Assistant Att'y Gen. of the United States) (stating that it is "not safe to assume" that a nonsuspect third party will comply with a subpoena because they will likely have a relationship making them loyal to, controlled, or influenced by a suspect, unless the third party is an "institutional record holder[]"); *Citizens Privacy Protection Act: Hearings on S. 3162 and S. 3164 Before the Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 95th Cong. 1–3 (1979) (statement of Sen. Birch Bayh) (introducing hearings on a previous bill proposed in response to *Zurcher* that would have protected against searches of materials "in possession of a person not implicated in criminal activity").

[29] *See* 42 U.S.C. § 2000aa (2006).

The form and scope of the Act's protections underwent multiple iterations. Notably, an early bill would have prohibited searches and seizures for documentary materials of those "engaged in first amendment activities."[30] The House subsequently deleted the phrase; the legislative history indicates that the change was borne of the ambiguous boundaries of the category "first amendment activities."[31] The edit foreshadowed what would become persistent confusion over the scope of protection afforded by the Act. Despite the change, Department of Justice officials supporting the bill clearly understood it as a "first amendment bill."[32] As Assistant Attorney General Philip Heymann testified, the Department still envisioned the bill to be "as broad as the first amendment, broader than [the] press or anything thought of as organized press," reaching "all first amendment rights," including "people who will never succeed in publishing, and those who publish every day."[33]

B. Requirements of the Act

As enacted, Subchapter I[34] of the Act institutes a general "no-search" rule protecting certain people.[35] Specifically, the Act prohibits law enforcement from searching materials in the possession of people who have "a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication."[36] Key to this portion of the Act is a person's intention to disseminate some form of "public communication." While this language clearly encompasses reporters, the legislative history suggests that "academicians, authors, filmmakers, and

---

[30] *See* S. REP. NO. 96-1003, at 7 (1980) (Conf. Rep.) (discussing the House amendment to change the title of S. 1790).

[31] *See id.* The "press" is similarly difficult to define. *See supra* note 14 and accompanying text.

[32] *See Privacy Protection Act Hearing*, *supra* note 27, at 33 (testimony of Philip B. Heymann, Assistant Att'y Gen. of the United States); *see also id.* at 44 ("If it is work product, we say, 'First amendment wins.' It will be a while before you hear us saying that again.").

[33] *Id.* at 32–33.

[34] § 2000aa. Subchapter II of the Act directs the Attorney General to issue guidelines governing how federal officers and investigators should obtain documentary materials possessed by third parties who are not suspects. *Id.* § 2000aa-11. The guidelines address the personal privacy interests of the person in possession of the materials, a requirement that the least intrusive method of obtaining the documents be used, a recognition of the special privacy interests posed by privileged relationships, and a warrant approval process. 28 C.F.R. §§ 59.1–.6 (2012).

[35] Some refer to Subchapter I of the Act as establishing a "subpoena-first" rule. *See* Jose M. Sariego, Note, *The Privacy Protection Act of 1980: Curbing Unrestricted Third-Party Searches in the Wake of* Zurcher v. Stanford Daily, 14 U. MICH. J.L. REFORM 519, 540–41 (1981). Sariego correctly notes that "any mechanism by which the party to be searched is notified of the impending search and allowed to object, including but not limited to subpoenas *duces tecum*, suffices to escape the Act's requirements." *Id.* at 541. To avoid making a narrower inference than the text demands, this Note uses the "no-search" rule label.

[36] § 2000aa(a).

free lance [sic] writers and photographers" are also protected.[37] The purpose of the resultant protection has been characterized as defending the flow of information to the public.[38]

The Act protects only certain materials from search and seizure: "work product" and "documentary materials."[39] Work product is defined as materials prepared "in anticipation of communicating such materials to the public," including "mental impressions, conclusions, opinions, or theories" of the material's creator.[40] Documentary materials are defined to include "photographs, . . . films, negatives, video tapes, audio tapes, and other mechanically, magentically [sic] or electronically recorded cards, tapes, or discs."[41] Neither work product nor documentary materials include "contraband or the fruits of a crime."[42]

Protection for each category of materials is subject to a complex set of exceptions and sub-exceptions.[43] Protection for work product, tied to the creator's mental process, is subject to just two exceptions.[44] The first "suspect" exception allows a search or seizure when the person in possession of the relevant materials is a suspect in the crime under investigation.[45] However, if the crime is the receipt or possession of the materials sought, the suspect exception does not apply unless the materials relate to national defense, classified information, or the sexual exploitation of children.[46] The second exception applies when immediate seizure is "necessary to prevent the death of, or serious bodily injury to, a human being."[47] The strong protection afforded work product (compared to that for documentary materials) may be due to the special regard Congress gave reporters' mental process.

Protection against search and seizure of documentary materials is subject to four exceptions.[48] The first two exceptions are identical to those the Act provides for work product.[49] Additionally, searches for

---

[37] H.R. REP. NO. 96-1064, at 5 (1980).

[38] *See* Sariego, *supra* note 35, at 535.

[39] § 2000aa.

[40] *Id.* § 2000aa-7(b).

[41] *Id.* § 2000aa-7(a) (footnote omitted).

[42] *See id.* § 2000aa-7(a), (b). Congress did not anticipate that documentary materials would often fall into this category. *See* S. REP. NO. 96-874, at 16 (1980) ("These traditional categories of things which are properly subjects for search are in a vast majority of instances not documentary materials, but rather money, guns, weapons, narcotics, etc.").

[43] For a plain-language explanation of the exceptions, sub-exceptions, and sub-sub-exceptions, see Eckenwiler, *supra* note 9, at 728.

[44] *See* Sariego, *supra* note 35, at 544 (citing S. REP. NO. 96-874, at 10).

[45] § 2000aa(a)(1).

[46] *Id.*

[47] *Id.* § 2000aa(a)(2).

[48] *Id.* § 2000aa(b).

[49] *Id.*

documentary materials are allowed in two other situations. First, documentary materials may be seized pursuant to a warrant when there is reason to believe that giving notice would result in the "destruction, alteration, or concealment" of the materials.[50] This exception is justified: the Act's purpose was to control *how* law enforcement officials obtained access to documentary materials, not to prevent their access altogether.[51] Second, documentary materials may be seized when they have not been produced in response to a court order after appellate remedies have been exhausted or there is reason to believe that delay would "threaten the interests of justice."[52]

The Act creates a civil cause of action for damages to enforce the prohibition on searches and seizures:

> A person aggrieved by a search for or seizure of materials in violation of this chapter shall have a civil cause of action for damages for such search or seizure . . . against the United States . . . or against any other governmental unit, all of which shall be liable for violations of this chapter by their officers or employees while acting within the scope or under color of their office or employment; and . . . against an officer or employee of a State who has violated this chapter . . . .[53]

Any person aggrieved by a violation of the Act may sue for damages in federal court.[54] The legislative history suggests that to be aggrieved, a person must possess the materials seized; people to whom the materials relate, but who are not in possession of them, were not to be able to sue,[55] though this may be a stricter reading of the text than courts apply in practice.[56] No matter the aggrieved party or amount of damages suffered, an officer has a complete defense where he or she "had a reasonable good faith belief" that the challenged conduct was lawful.[57] Sparse case law has emerged from this private right of action to guide courts' and law enforcement officers' interpretations of the Act.

---

[50] *Id.* § 2000aa(b)(3).

[51] *See Privacy Protection Act Hearing*, *supra* note 27, at 6 (testimony of Sen. Max Baucus) ("[T]he only question is how authorities should go about obtaining these materials . . . .").

[52] § 2000aa(b)(4).

[53] *Id.* § 2000aa-6(a).

[54] *Id.* § 2000aa-6(h).

[55] *See* S. REP. NO. 96-874, at 14 (1980) ("It is not the intent . . . to expand current law concerning which persons have standing to bring an action for an unlawful search or seizure. Thus, . . . it would be the person in possession of the materials, and not the party to whom the information related—the criminal suspect—who would have standing to bring an action under these provisions."). This is a stricter reading of the text than courts apply in practice. *See infra* note 79 and accompanying text.

[56] *See, e.g.*, Guest v. Leis, 255 F.3d 325, 341 (6th Cir. 2001) (interpreting "aggrieved person" to include users of an online bulletin board service who were not in physical possession of the material seized by analogizing to provisions in the Electronic Communications Privacy Act (ECPA)); *see also infra* note 79 and accompanying text.

[57] § 2000aa-6(b).

C. Subsequent Interpretations of the Act

Courts have not had many occasions to interpret the Act. Few people have brought suit under its provisions; still fewer cases have reached the circuit courts. It is difficult to know the reason for the lack of suits. People may not know of their eligibility to sue; law enforcement officers violating the Act's provisions are unlikely to simultaneously notify citizens of the private right of action it confers. Most courts considering cases brought under the Act identify an early reason to deny the claim amongst its complex web of exceptions (especially the potent and sweeping suspect exception),[58] find no reason to believe that a person intended to disseminate information to the public,[59] or dismiss the claims on technical grounds.[60]

Those courts interpreting provisions of the Act have similarly avoided identifying the outer contours of its protections. Instead, courts have tailored their decisions to ancillary issues, such as the limits of protection for certain kinds of publishers,[61] the privacy rights of users of online bulletin board systems,[62] and the absence of required statutory procedures for obtaining a warrant.[63] Cases interpreting the Act have involved seizures of computing equipment that stored information from people who ran

---

[58] *See, e.g.*, S.H.A.R.K. v. Metro Parks Serving Summit Cnty., 499 F.3d 553, 566–67 (6th Cir. 2007) (applying suspect exception); Pinnavaia v. FBI, 218 F. App'x 646, 647 (9th Cir. 2007) (affirming a dismissal where the plaintiff conceded that he was a suspect when the challenged search took place); Benson v. United States, Nos. 94-4182, 95-4061, 1995 WL 674615, at *2–3 (10th Cir. Nov. 13, 1995) (affirming the district court's holding that the Privacy Protection Act did not apply because the plaintiffs were suspects and the information seized did not fall within the communication exception).

[59] *See, e.g.*, Teichberg v. Smith, 734 F. Supp. 2d 744, 752 (D. Minn. 2010) (granting summary judgment in favor of law enforcement officials when the plaintiff, a photographer, failed to demonstrate an issue of fact regarding whether the officers believed the photographer had a purpose to disseminate information to the public); Lambert v. Polk Cnty., 723 F. Supp. 128, 132 (S.D. Iowa 1989) (noting, in the context of a motion for a preliminary injunction, that there was no reason that officers should have believed that a person who recorded a fight on video intended to distribute it to the public).

[60] *See, e.g.*, Mink v. Suthers, 482 F.3d 1244, 1257–58 (10th Cir. 2007) (affirming a dismissal for failure to state a claim where the plaintiff failed to name the individuals who participated in the search and seizure and failed to allege that the defendant district attorney "directed, controlled or participated in the search or seizure"); United States v. Any & All Radio Station Transmission Equip., 218 F.3d 543, 551 (6th Cir. 2000) (affirming the district court in finding that radio transmission equipment is not documentary or work product material subject to protection under the Act).

[61] *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 440 (W.D. Tex. 1993), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

[62] *See* Guest v. Leis, 255 F.3d 325, 341–42 (6th Cir. 2001) (holding that users of bulletin board systems could be "aggrieved" under the Act so as to have a cause of action). Bulletin board systems (BBSes) were early collaborative tools that allowed people to connect using a modem and phone line to read and share messages, pictures, and other files. Modeled after corkboard bulletin boards, BBSes were popular with hackers—including many committed to free speech online. *See Bulletin-Board Systems*, *in* ENCYCLOPEDIA OF NEW MEDIA 45–48 (Steve Jones ed., 2003) (calling the early 1990s the "'golden years' of BBSing"); *Bulletin Board Systems (BBS)*, *in* ENCYCLOPEDIA OF COMPUTER SCIENCE AND TECHNOLOGY 61–62 (Harry Henderson ed., rev. ed. 2009).

[63] *See* Citicasters, Inc. v. McCaskill, 883 F. Supp. 1282, 1288 (W.D. Mo. 1995), *rev'd*, 89 F.3d 1350 (8th Cir. 1996).

online bulletin board systems (BBSes), the precursors to modern online communication services.[64] In these cases, the courts could have explicated the statute's breadth as applied to such computing environments. However, these cases do not help settle the Act's ambiguities; one relies on narrow facts to avoid questions posed by computers, and the other pairs contradictory holdings on standing and commingled protected and unprotected materials to deny much protection at all.

The first such case began when the Western District of Texas applied the Act to a claim arising from the execution of a search warrant on Steve Jackson Games, a publisher of books, magazines, and games, and the host of the online bulletin board system Illuminati.[65] The search warrant stemmed from an incident in which a security director reported that a computer hacker had accessed BellSouth's 911 emergency system and published the 911 program on a public online bulletin board. Following the report, the Secret Service collected information that it thought tied the hack to an employee of Steve Jackson Games.[66] In the course of its investigation, the Secret Service erroneously concluded that Steve Jackson Games' BBS also published criminal hacker materials.[67] However, the Secret Service had in fact mistaken a manual for a hacker-themed online role playing game to be a "manual for computer crime."[68]

Based on this erroneous belief, the Secret Service then obtained and executed a search warrant on the corporate office of Steve Jackson Games. Agents seized, amongst other things, the computer that hosted both the bulletin board system and drafts of game-related materials meant for publication.[69] The Secret Service retained the seized material for over three months, despite the company's complaints that its publishing business was interrupted.[70] Afterward, Steve Jackson Games, Steve Jackson, and three employees sued the Secret Service, alleging that the Secret Service had violated the Privacy Protection Act in addition to two other statutory provisions.[71] The court acknowledged that the game publisher fell within

---

[64] Julian Sanchez, *The Prehistory of Cyberspace: How BBSes Paved the Way for the Web*, REASON.COM (Dec. 1, 2005, 12:00 AM), http://reason.com/archives/2005/12/01/the-prehistory-of-cyberspace.

[65] *See Steve Jackson Games*, 816 F. Supp. at 434.

[66] *Id.* at 435.

[67] *Id.* at 436.

[68] *See* Suzanne Stefanac, *Dangerous Games*, CAL. LAW., Oct. 1994, at 56, 60; *see also SJ Games vs. the Secret Service*, STEVE JACKSON GAMES, http://www.sjgames.com/SS (last visited May 25, 2013) ("They seemed to make no distinction between a discussion of futuristic credit fraud, using equipment that doesn't exist, and modern real-life credit card abuse. A repeated comment by the agents was 'This is real.'").

[69] *Steve Jackson Games*, 816 F. Supp. at 439–40.

[70] *Id.* at 437.

[71] *Id.* at 434. During the three months without the seized materials and equipment, Steve Jackson Games claimed a total of over $150,000 in out-of-pocket expenses, lost sales, and lost profits. *Id.* at 438.

the scope of the Privacy Protection Act, noting that "[w]hile the content of these publications are not similar to those of daily newspapers, news magazines, or other publications," the material was protected.[72] Steve Jackson Games won a damages award because the Secret Service violated the Act by illegally seizing publishable documents.[73] However, the court's ruling avoided actually deciding whether seizure of the computers storing the e-mail and bulletin board systems violated the Act. Instead, the court based its holding on the fact that the Secret Service refused to return printed drafts of the book *Gurps Cyberpunk*, which was clearly classified as work product under the Act.[74] By resting its decision on facts tied to physical materials, the court avoided resolving ambiguity over how the Act protects the computing equipment also seized in the incident.

The second bulletin board system case, *Guest v. Leis*, more directly confronted questions posed by computer searches.[75] *Guest* arose from the seizure of two bulletin board systems during an obscenity investigation by the Hamilton County, Ohio, Regional Electronic Computer Intelligence Task Force.[76] Users of one system filed a class action on behalf of subscribers alleging violations of the Privacy Protection Act, the First and Fourth Amendments, the Electronic Communications Privacy Act, and state law; alleging the same claims, the users, system operator, and computer owner filed suit in relation to the other system.[77] After the district court granted summary judgment for the defendants in each case, the plaintiffs appealed.

The Sixth Circuit found that the plaintiffs had standing because they were "aggrieved"[78] under the Privacy Protection Act, even though another person may have been in possession of the materials seized.[79] In so holding,

---

[72] *Id.* at 434 n.1, 441.

[73] *Id.* at 441, 443 (awarding $8781 in expenses and $42,259 in compensatory damages). The court also awarded damages under the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. §§ 2701–2712 (2006), for the seizure of a computer containing stored e-mail, *Steve Jackson Games*, 816 F. Supp. at 442–43, and held that the Secret Service did not violate the Federal Wiretap Act, *id.* at 442. *See also* Nicole Giallonardo, Casenote, Steve Jackson Games v. United States Secret Service*: The Government's Unauthorized Seizure of Private E-Mail Warrants More than the Fifth Circuit's Slap on the Wrist*, 14 J. MARSHALL J. COMPUTER & INFO. L. 179 (1995) (criticizing the Fifth Circuit for upholding the district court's ruling that there was no violation of the Wiretap Act).

[74] *Steve Jackson Games*, 816 F. Supp. at 438–39.

[75] *See* 255 F.3d 325 (6th Cir. 2001).

[76] *Id.* at 329–30.

[77] *Id.* at 330.

[78] 42 U.S.C. § 2000aa-6(a) (2006) ("A person aggrieved by a search for or seizure of materials in violation of this chapter shall have a civil cause of action for damages . . . .").

[79] *Guest*, 255 F.3d at 341 (citing the Electronic Communications Protection Act, 18 U.S.C. § 2510(11) (2000) (defining "aggrieved person" as "a person who was a party to any intercepted wire, oral, or electronic communication or a person against whom the interception was directed")). The appellants had argued that the users were in "joint possession" of the contents of the bulletin board system because they "retained control over the messages they posted, having the ability to create, edit,

the court rejected the argument that only the operator in possession of the materials could have a cause of action, not mere users of the BBS.[80] The court then addressed the difficulties posed by computer searches, "a situation unforeseen by the drafters."[81] The court noted that the Act does not "explicitly address" liability for seizing "communicative material that is technically difficult to separate" from evidence of a crime.[82] To prevent criminals from too easily "insulat[ing]" their criminal records and avoid impeding law enforcement, the court held that officials could seize protected materials commingled with unprotected evidence on a suspect's computer.[83] The court warned police not to *search* protected materials, but it failed to specify how a computer search should be conducted to comply with such a limitation.[84]

The last notable challenge under the Act that reached the circuit level explored warrant procedure. In *Citicasters v. McCaskill*, the Eighth Circuit considered whether specific steps are required during a warrant application when an exception to the Act's no-search rule applies.[85] Specifically, the court addressed the question of who must decide if an exception applies before a court issues a warrant for a search. Reversing the district court, the Eighth Circuit held that a neutral magistrate need not decide the question.[86] Furthermore, the court held that a warrant application need not disclose applicable exceptions for it to issue.[87] Congress's silence informed the court's reasoning. The Act's lack of a specified warrant procedure indicated "congressional appreciation of the proper restraints of federalism" with regard to state procedures governing how state law enforcement officials acquire warrants.[88] In dissent, Judge Bright disagreed that the Act's text provided a clear answer to the question.[89] Finding that the statute's silence[90] required consideration of the legislative history and

---

and send private messages or publish materials publicly." Reply Brief of Appellants at 23, *Guest*, 255 F.3d 325 (No. 99-4115), 2000 WL 35462790.

[80] *See Guest*, 255 F.3d at 341 ("Defendants argue that most of the plaintiffs lack standing in these cases because only the operator of the bulletin board systems 'possessed' the materials at issue in these cases.").

[81] *Id.*

[82] *Id.* at 342.

[83] *Id.*

[84] *See id.*

[85] 89 F.3d 1350 (8th Cir. 1996).

[86] *See id.* at 1355–56 ("Where Congress has provided a specific means for achieving its purpose, we must . . . not embellish its legislative scheme with additional procedural innovations.").

[87] *Id.* at 1356.

[88] *Id.* at 1355 n.6. The majority found the statutory silence to clearly and unambiguously indicate the correct meaning of the statute and declined to consider legislative history. *See id.* at 1354–55.

[89] *Id.* at 1357 (Bright, J., concurring in part and dissenting in part).

[90] *Id.* at 1357–58.

purpose,[91] Judge Bright ultimately criticized the majority because "[a]fter-the-fact review can only punish violation, not prevent it."[92]

These cases, while small in number, highlight the difficulties courts face and avoidance strategies that they exercise when applying the Act to modern environments rich in computing. The resulting law would veer toward underprotection if courts followed these examples. Courts allow warrants to be issued without requiring officials to specify what exceptions to the Act exist. Seizure of commingled materials continues where technology simply presents a difficult question and courts allow law enforcement to seize laptops, phones, and servers. Broad changes in the information industry have led to severely weakened statutory protection for software companies and publishers whose products and communications are entirely digital. Specifically, increasingly ubiquitous self-publishing services and low barriers to entering the app economy equip more people than ever before to readily disseminate information to the public—at which point they should receive protection under the Act.

II. INTERVENING CHANGES IN THE INFORMATION INDUSTRY

Congress passed the Privacy Protection Act in an era that preceded explosive growth in the computing and information industry.[93] Since 1980, two trends in particular typify the changes that have fundamentally altered the landscape to which the Act may apply: mobile application services for smartphones and online self-publishing. The transformation of publishing, expansion of mobile service providers, and increasing ubiquity of content pushed to subscribers' mobile devices has led to a growth in app-driven services.[94] The Pew Internet and American Life Project estimates that by May 2013, 56% of American adults had smartphones;[95] usage has steadily climbed.[96] These include information-rich services from major multi-platform publishers[97] as well as apps that may arguably serve to replace the functions of traditional media such as books.[98] This trend invites the

[91] *Id.* at 1359–60.

[92] *Id.* at 1360 (citing 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 4.3(a), at 459 (3d ed. 1996)).

[93] *See* Eckenwiler, *supra* note 9.

[94] *See, e.g.*, *Insights on the Emerging Mobile App Economy*, NIELSEN (Sept. 14, 2010), http://www.nielsen.com/us/en/newswire/2010/insights-on-the-emerging-mobile-app-economy.html.

[95] *See Device Ownership: Trend Data (Adults)*, PEW INTERNET, http://www.pewinternet.org/Static-Pages/Trend-Data-(Adults)/Device-Ownership.aspx (last visited May 25, 2013).

[96] *See id.* (showing smartphone adoption rates rising from 2011 to 2013).

[97] *See, e.g.*, *The New York Times Mobile*, N.Y. TIMES, http://www.nytimes.com/services/mobile/apps (last visited May 25, 2013).

[98] *See, e.g.*, Julia Moskin, *The Cooking App Comes Into Its Own*, N.Y. TIMES, Nov. 9, 2011, at D1 (suggesting that tablet-based cooking apps may diminish the use of printed cookbooks).

question: are all information providers in this new "app economy"[99] protected by the Act because they disseminate information to the public?

The transformation of communications has not been a one-way street. While commercial information service providers have exploded, individuals also increasingly publish online without their content being mediated by a publisher.[100] Online self-publishing is more than just an extra option for those seeking to publish news, books, and other such resources. For many, it is a core daily communication practice. Recent studies show that 85% of adults and 95% of teens in the United States go online on at least an occasional basis, a majority of whom post original content.[101]

Questions again emerge from this trend: does the Privacy Protection Act protect all who communicate online, blogger and reporter alike?[102] Furthermore, if the Act applies to these activities, which digital materials garner its protection? Finally, which interests does the Act protect? In a historical press context, the answers to these questions are relatively clear. Privacy interests of confidential sources, reporters' interests in publishing their work, and a press operation's overall interest in continuity would all arguably trigger the motivation behind the Act.[103] The modern press context, employing many bloggers alongside copy editors and print

---

[99] For a summary, see NIELSEN CO., THE STATE OF MOBILE APPS (2010), *available at* http://www.nielsen.com/us/en/reports/2010/The-State-Of-Mobile-Apps.html.

[100] *See, e.g.*, Geoffrey A. Fowler & Jeffrey A. Trachtenberg, *'Vanity' Press Goes Digital*, WALL ST. J., June 3, 2010, at A1; Elinor Mills, *Self-Publishing Made Easy Online*, CNET NEWS (Jan. 9. 2007, 4:00 AM), http://news.cnet.com/Self-publishing-made-easy-online/2100-1038_3-6148342.html. Readers curious to begin their own self-publishing operation should see Scott Steinberg, *How To: Self-Publish Anything Online*, MASHABLE (Aug. 5, 2010), http://mashable.com/2010/08/05/self-publish-anything.

[101] *See Who's Online: Internet User Demographics: Trend Data (Adults)*, PEW INTERNET, http://pewinternet.org/Trend-Data-(Adults)/Whos-Online.aspx (last visited May 25, 2013); *Teen Internet User Demographics: Trend Data (Teens)*, PEW INTERNET, http://pewinternet.org/Trend-Data-(Teens)/Whos-Online.aspx (last visited May 25, 2013). While multiple news outlets have reported a decline in the rates of people blogging, the decrease is usually described as offset by a corresponding increase in use of social media or microblogging services such as Twitter. It does not indicate a decrease in online self-publishing. *See* Verne G. Kopytoff, *Blogs Wane as the Young Drift to Sites like Twitter*, N.Y. TIMES, Feb. 21, 2011, at B1; Ryan Singel, *Blogging 'Peaks,' but Reports of Its Death Are Exaggerated*, WIRED (Dec. 16, 2010, 3:10 PM), http://www.wired.com/epicenter/2010/12/long-live-blogging.

[102] Some argue that it does, but the question has not been definitively settled by the courts. *See* Adam Cohen, *The Media that Need Citizens: The First Amendment and the Fifth Estate*, 85 S. CAL. L. REV. 1, 47 (2011) ("The statute's protection of 'similar forms' gives courts a textual hook for protecting bloggers and other new media, but it is not clear how willing they are to do so."). Cohen noted the 2010 search of a Gizmodo blogger as highlighting the salience of this ambiguity. *Id.* at 48; *see also* Lyrissa Lidsky, *Search of Gizmodo Journalist's "Newsroom"/Bedroom: Federal Law*, PRAWFSBLAWG (Apr. 26, 2010, 9:53 PM), http://prawfsblawg.blogs.com/prawfsblawg/2010/04/search-of-gizmodo-journalists-newsroombedroom.html.

[103] Each interest is indeed bound up in the simple observation that "the promise of nondisclosure is necessary for many types of news gathering." Branzburg v. Hayes, 408 U.S. 665, 731 (1972) (Stewart, J., dissenting).

foremen, shows how the line has blurred.[104] For a blogger or app developer, which interests are protected by the Act could mean the difference between its protections being triggered or not. Operational continuity may not be an issue for a blogger who has many options for where to connect to the Internet and from what computing device she might publish. Protecting the privacy of third-party customers could mean that the Act should prevent searches and seizures of the devices of an app developer. The next Part addresses ambiguities of the Act that emerge in light of these technological transformations.

III. RESOLVING STATUTORY AMBIGUITIES TO INFORM ENFORCEMENT

In light of these changes, consistent enforcement of the Act demands resolution of its ambiguities. First, given the ubiquity of personal computing and the commonplace nature of self-publishing, we must examine who is protected by the Act. Second, the rise in personal computing leads to questions about what materials and information are protected as work product or documentary materials. Moreover, how are devices and equipment that house both protected and unprotected data protected? Lastly, given the hazy boundaries between speech, privacy, and the press, clarifying what interests the Act protects will help guide how it should be enforced today.

To resolve these three ambiguities, the first step is, of course, to consider whether the text of the Act itself demands a particular result.[105] If it does not, then a practical reasoning approach considers the cogency and relative merits of other arguments.[106] In addition to such traditional

---

[104] *See* Glik v. Cunniffe, 655 F.3d 78, 84 (1st Cir. 2011) ("[C]hanges in technology and society have made the lines between private citizen and journalist exceedingly difficult to draw. The proliferation of electronic devices with video-recording capability means that many of our images of current events come from bystanders with a ready cell phone or digital camera rather than a traditional film crew, and news stories are now just as likely to be broken by a blogger at her computer as a reporter at a major newspaper.").

[105] *See, e.g.*, McNeill v. United States, 131 S. Ct. 2218, 2221 (2011) ("As in all statutory construction cases, we begin with 'the language itself [and] the specific context in which that language is used.'" (alteration in original) (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997))); Dean v. United States, 556 U.S. 568, 572 (2009) (quoting Williams v. Taylor, 529 U.S. 420, 431 (2000)). Even scholars who promote using a more varied toolbox in statutory interpretation recognize that the role of clear statutory text is paramount. *See, e.g.*, William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1496 (1987) ("In many cases, the text of the statute will provide determinate answers . . . .").

[106] *See* William N. Eskridge, Jr. & Philip P. Frickey, *Statutory Interpretation as Practical Reasoning*, 42 STAN. L. REV. 321, 322 n.3, 323 (1990) ("By 'practical reason,' we mean an approach that eschews objectivist theories in favor of a mixture of inductive and deductive reasoning (similar to the practice of the common law), seeking contextual justification for the best legal answer among the potential alternatives."). This Note follows Professors Eskridge and Frickey in avoiding a foundationalist theory of statutory interpretation—that is, one prioritizing the text, intent, or purpose of a statute above all other sources of interpretation. *See id.* at 321. The vast literature on the relative merits of different schools of thought on statutory interpretation cannot be covered in full here, but see,

approaches to statutory interpretation, Professor Daniel Solove's theory of the First Amendment as criminal procedure is a useful model for analyzing the Act's three ambiguities and evaluating how best to interpret it to achieve its objectives.[107]

A. Solove's First Amendment as Criminal Procedure

Professor Solove is critical of the existing relationship between the First Amendment and criminal procedure. Finding modern Fourth and Fifth Amendment jurisprudence insufficient to protect First Amendment values,[108] he proposes that the First Amendment "serve as an independent source of [criminal] procedure," similar to the Fourth Amendment, "to protect expressive and associational activity from government information gathering."[109] The fact that Solove's theory has not been adopted as constitutional law does not lessen its utility for exploring differing interpretations of how this statute should operate.[110] In fact, the principles he sets out uniquely inform statutory construction of the Act given its roots in First Amendment theory.[111]

Solove suggests a two-part inquiry to trigger First Amendment protections. First, to determine whether the government action affects activities that fall within the boundaries of the First Amendment, Solove suggests inquiring into whether it interferes with expressive activity protected by First Amendment values.[112] First Amendment values arise when communication, association, or other activities "implicate belief,

---

for example, WILLIAM N. ESKRIDGE, JR., PHILIP P. FRICKEY & ELIZABETH GARRETT, CASES AND MATERIALS ON LEGISLATION: STATUTES AND THE CREATION OF PUBLIC POLICY 689–846 (4th ed. 2007); KENT GREENAWALT, LEGISLATION: STATUTORY INTERPRETATION (1999); and ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW (Amy Gutmann ed., 1997).

[107] *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007) (proposing that the First Amendment serve as an independent source of constitutional criminal procedure).

[108] *See id.* at 132–42 (chronicling the development of Fourth and Fifth Amendment protections and the gradual lessening of protections related to the First Amendment afforded by Fourth Amendment jurisprudence).

[109] *Id.* at 151.

[110] It may not be a viable position for a court to adopt post-*Zurcher*. *Cf.* City of Boerne v. Flores, 521 U.S. 507, 535–36 (1997) ("Our national experience teaches that the Constitution is preserved best when each part of the Government respects both the Constitution and the proper actions and determinations of the other branches. When the Court has interpreted the Constitution, it has acted within the province of the Judicial Branch, which embraces the duty to say what the law is. When the political branches of the Government act against the background of a judicial interpretation of the Constitution already issued, it must be understood that in later cases and controversies the Court will treat its precedents with the respect due them under settled principles, including *stare decisis*, and contrary expectations must be disappointed." (citation omitted)).

[111] *See, e.g.*, *Privacy Protection Act Hearing*, *supra* note 27, at 51 (prepared statement of Philip B. Heymann, Assistant Att'y Gen. of the United States).

[112] *See* Solove, *supra* note 107, at 153 (adopting the approach recommended in Robert Post, *Recuperating First Amendment Doctrine*, 47 STAN. L. REV. 1249, 1255 (1995)).

discourse, or relationships of a political, cultural, or religious nature."[113] Next, Solove suggests that First Amendment procedural protections are warranted only where a "discernable 'chilling effect'" is at risk.[114] The risk of a chilling effect is high when associational behavior is at issue or when a person is writing, purchasing, or consuming information such as that in a book or on a website.[115] Where either of these two elements are present, Solove would require (1) the government to demonstrate a significant interest in the information sought and (2) that the manner of collection be narrowly tailored to achieve that interest.[116] Usually these requirements would be met by the use of a warrant acquired after an affirmative showing of probable cause.

First Amendment rights often operate as a defense in criminal litigation.[117] The Act's private right of action thus presents an unusually affirmative posture through which to analyze speech-related rights as they intersect with the information-gathering procedures of law enforcement. Solove's framework has previously proven useful in analyzing intersections between the First Amendment and statutory law governing compelled disclosure.[118] Here, it serves as an aid in sorting out the proper (and ideal) scope of the Act, as well as the implications of competing interpretations of the Act's ambiguities.

B. Ambiguity One: The Protected Population

The first ambiguity is the question of to whom the Act applies. In light of developments in online publishing,[119] it is necessary to determine whether the Act should reach so far as to protect all digital content providers and people who publish online or whether the Act has a more limited reach. The text of the Act is very broad, preventing the search or seizure of "any work product materials" possessed by someone with a "purpose to disseminate to the public" a "form of public communication."[120] As long as what a person intends to disseminate is "a newspaper, book, [or] broadcast" or falls under the broad umbrella of

---

[113] *See* Solove, *supra* note 107, at 153.

[114] *Id.* at 154.

[115] *See id.* at 156.

[116] *See id.* at 159, 161.

[117] *See* Jennifer E. Laurin, *Rights Translation and Remedial Disequilibration in Constitutional Criminal Procedure*, 110 COLUM. L. REV. 1002, 1075 (2010).

[118] *See* Thomas P. Crocker, *The Political Fourth Amendment*, 88 WASH. U. L. REV. 303, 345 n.238 (2010) (contrasting the First and Fourth Amendment models of protecting liberties); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 795, 812, 814 (2008) (using Solove's framework to analyze associational interests implicated in searches and seizures).

[119] *See supra* Part II.

[120] 42 U.S.C. § 2000aa(a) (2006).

"similar form[s] of public communication,"[121] a plain-text reading of the statute applies. At first glance, both a blogger and an app developer appear to be protected by a plain-text reading of the Act.

The legislative history supports this broad reading of the clause. Assistant Attorney General Philip Heymann testified that the Act protects everyone holding materials connected with "First Amendment activities," rather than solely the institutional press.[122] The principle debate during enactment was over scope;[123] legislators focused on the singular question of whether the Act should provide broad third-party nonsuspect protection[124] or whether it was better to enact—as Congress ultimately did—a more limited "First Amendment" bill.[125] Bloggers and app developers post and distribute content in the exercise of their speech rights and thus should be protected under a First Amendment understanding of the Act.

Defining the protected population that broadly, though, risks hampering law enforcement's ability to search anyone with a home computer or smartphone. A more limited construction of the statute could be found by construing the meaning of "a newspaper, book, broadcast, or other similar form of public communication" to be limited to information produced by media institutions for broad public consumption.[126] Furthermore, each is often a form of investment-backed contribution to a sector of the information industry. Such a construction of the list may not allow "similar form[s] of public communication"[127] to encompass personal communication, such as that of a noncommercial blogger. This distinction may ultimately be insignificant or even unworkable, given the blurry line between "news" as an investment-backed industry and the "news" broken by self-publishing individuals.[128]

One might thus use this approach to limit the Act to protecting only a narrow subset of those people involved in information dissemination, such

---

[121] *Id.*

[122] *Privacy Protection Act Hearing*, *supra* note 27, at 51 (prepared statement of Philip B. Heymann, Assistant Att'y Gen. of the United States).

[123] *See Privacy Protection Act Hearing*, *supra* note 27, at 5 (remarks of Sen. Birch Bayh) (listing bills with varying subjects of protection); *see also* Erburu, *supra* note 28, at 163–73 (contrasting the "press-only" and "third-party" bills considered by the Ninety-sixth Congress); Elizabeth H. Sillin, Note, Citicasters v. McCaskill*: Probing the Privacy Protection Act of 1980*, 20 W. NEW ENG. L. REV. 437, 470 (1998) (noting the lack of debate on required warrant procedures).

[124] *See* Erburu, *supra* note 28, at 163–73 (describing the "third-party" bills considered by the Ninety-sixth Congress).

[125] *See Privacy Protection Act Hearing*, *supra* note 27, at 32–33 (testimony of Philip B. Heymann, Assistant Att'y Gen. of the United States).

[126] *Noscitur a sociis* instructs that "words grouped in a list should be given related meaning." Dole v. United Steelworkers of Am., 494 U.S. 26, 36 (1990) (quoting Massachusetts v. Morash, 490 U.S. 107, 114–15 (1989)).

[127] 42 U.S.C. § 2000aa (2006).

[128] *See* Glik v. Cunniffe, 655 F.3d 78, 84 (1st Cir. 2011) (highlighting the blurry outer boundaries of the news industry).

as commercial publishing or broadcasting. However, construing statutory language is not merely an exercise in ascertaining "the outer limits of [a phrase's] definitional possibilities."[129] Furthermore, should a court follow the rationale of the Fifth Circuit in protecting a game publisher, the literal words of the Act do not afford this limitation.[130] Given the broad language of the Act, the apparent congressional intent to protect activities ranging the full extent of the First Amendment, and the weaknesses inherent in forcing more limited constructions,[131] the soundest reading of the Act seems to extend as far as the First Amendment—the label removed from earlier bills—to protect all people who communicate to the public.[132]

Solove offers a constitutionally based limiting principle. His focus on expressive activities that implicate "belief, discourse, or relationships of a political, cultural, or religious nature" offers a functional way of sorting people who warrant more stringent protection from governmental intrusion from those for whom government inquiry does not necessarily trigger First Amendment restrictions.[133] Under this limitation, the blogger would more than likely warrant protection. The case is not so clear for the app developer. If the content of the app is business information, such as stock or finance quotes, one might conclude that the service does not implicate "belief, discourse, or relationships."[134] If, however, the relevant app publishes serial essays from an entrepreneurial Dickens-like developer, Solove's distinction may favor the app developer, too. Hinging protection on the type of content trips up the distinction, as bloggers and app developers alike are sure to confound the question of what constitutes "belief, discourse, or relationships of a political, cultural, or religious nature."

---

[129] Dolan v. U.S. Postal Serv., 546 U.S. 481, 486 (2006).

[130] *See* Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 434 n.1, 441 (W.D. Tex. 1993) ("While the content of [a game publisher's] publications are not similar to those of daily newspapers, news magazines, or other publications usually thought of by this Court as disseminating information to the public, these products come within the literal language of the Privacy Protection Act."), *aff'd*, 36 F.3d 457 (5th Cir. 1994); *see also* Leslie G. Berkowitz, *Computer Security and Privacy: The Third Wave of Property Law*, COLO. LAW., Feb. 2004, at 57, 64 ("[E]ven a BBS with relatively few subscribers is a 'publisher' under the PPA, as long as the BBS and its files are used, as they invariably are, for public communication.").

[131] *Cf.* FCC v. AT & T Inc., 131 S. Ct. 1177, 1184 (2011) (pointing out that AT & T failed to offer a sound reason from the text or context of a statute to disregard the ordinary meaning of the phrase "personal privacy").

[132] *But see supra* note 110 and accompanying text.

[133] Solove, *supra* note 107, at 153 (noting that the Supreme Court has recognized certain expression is "less central to, or not protected at all by, the First Amendment," such as "[o]bscenity, fighting words, and child pornography" (footnotes omitted)).

[134] Using the nature of the expression to inform the level of protection afforded by the Act in this way risks turning the original motivation for the Act—protecting news organizations—on its head. *See Privacy Protection Act Hearing*, *supra* note 27, at 1–2 (statement of Sen. Edward M. Kennedy) (describing the origins of the Act).

Making finer distinctions based on First Amendment values, which may themselves be contested, thus seems more problematic than a straightforward, if broad, textual reading of the Act. The inquiry grows more complex when we consider the range and hierarchy of digital information that law enforcement officials seek to seize. The next section examines which materials are protected under a broad reading of the Act that reaches all First Amendment actors.

C. Ambiguity Two: The Protected Materials

Defining what materials are protected could also be a straightforward task under the text of the Act, though a strict textual reading risks practical problems for law enforcement.[135] Two ambiguities cloud how the Act protects digital materials. First, because digital files that are housed en masse may rely collectively on services that run on a single server, it is important to determine at what level of "container" the Act's protections operate: file, device, or both. If individual files are protected but not the device on which they are stored, then the Act offers a very different level of protection than if blanket container-level protection applies. Second, if only file-level protection is offered, protecting files commingled with unprotected files poses a challenge for law enforcement officials and the courts to offer varied protection without eviscerating the Act.

The Act's text focuses on form and format in defining protected materials.[136] By defining exceptions based on whether material sought is work product or documentary materials, the statute's text connotes the press or any activity that similarly involves research, drafting, and preparation for publication. Work product and documentary materials are textually expansive for different reasons. Work product is not defined to include only specific formats; therefore, print, electronic, and other types of information all qualify. Likewise, by tying documentary materials to a container-level definition—"cards, tapes, or discs"—it is possible that any files stored on or in such a device are protected. However, the Sixth Circuit in *Guest* already rejected enforcing such a blanket container-protection rule for seizure of commingled protected and unprotected materials because it would allow criminals to insulate their contraband files with protected content.[137] By adopting a rule disallowing protection for "commingled" files on or in one digital container, the court framed its ruling as a solution for when protected digital content is "technically difficult to separate from the evidence of a crime whose seizure is authorized by a valid warrant."[138]

---

[135] *See* Guest v. Leis, 255 F.3d 325, 341–42 (6th Cir. 2001) (noting the difficultly of separating unprotected digital contraband from protected files).

[136] *See* 42 U.S.C. § 2000aa (2006); *see also* Anderson, *supra* note 14, at 436 (characterizing the Act's focus on form and format as "[t]ypical[]").

[137] *Guest*, 255 F.3d at 341–42.

[138] *Id.* at 342.

In the process, though, the Sixth Circuit ignored statutory text and effectively eliminated protection for documentary materials where digital containers store many files. In essence, the Sixth Circuit canceled out the Act's applicability in any situation in which law enforcement officials encounter a disc, drive, or server.

The *Guest* decision is unsatisfying in its inconsistency. The court also found that a user of a bulletin board—someone arguably not in physical possession of the seized equipment and files—was "aggrieved" under the Act.[139] This step was generous in defining the potential protectable interest and materials.[140] The court juxtaposed this generosity with its unforgiving imposition of the "commingling" rule,[141] cutting off liability for an improper search or seizure so long as contraband is alleged to be stored on one of the "containers" seized.

The first step of the court's analysis hints at an understanding of the Act's protections in line with Solove's framework. After all, if one's personal records are in the possession of a third party, those records enjoy little protection from the Fourth or Fifth Amendments even though they implicate First Amendment values.[142] As a quasi-constitutional "First Amendment" statute, the Act should protect such materials. However, the court's second analytical move fails these interests by allowing all files to be seized in the presence of a single file to which a statutory exception applies. The understanding of protected digital materials most in line with the text of the statute and broad First Amendment values would protect both the container and individual files relating to a potential aggrieved person.[143] Making distinctions based on the quality of communication or type of materials necessarily implicates the question of what interests are protected by the Act. The next section considers what interests the Act arguably serves to protect to justify this broad reading and identifies statutory weaknesses that can be solved if not by interpreting the Act, then by other mechanisms explored in Part IV.

D. Ambiguity Three: The Protected Interests

The Act does not announce policy objectives, nor does it include congressional findings.[144] However, its protections can be linked to more than one conceptually distinct protectable interest. Taken literally, the Act

---

[139] *Id.* at 341.

[140] One critic argues that such a "vicarious concern for governmental misuse of privately collected information[] seems an inferior concern." Clemens P. Work, *Whose Privacy?*, 55 MONT. L. REV. 209, 231 (1994).

[141] *Guest*, 255 F.3d at 342.

[142] *See* Solove, *supra* note 107, at 125.

[143] *Cf.* Fenno, *supra* note 11 ("[I]t appears facially that nearly everyone posting messages on the Internet or with online services is covered by the Act.").

[144] *See* 42 U.S.C. §§ 2000aa to 2000aa-12 (2006).

protects a person who intends to disseminate information to the public from searches or seizures of their work product or documentary materials.[145] That analysis is of little use to develop an informed resolution of the Act's ambiguities.[146] Even so, protected interests may stem from the Act's purpose,[147] so an inquiry into the motivation for the statute is relevant to determine what (and whose) interests should be protected.

As a response to *Zurcher*, the Act's presumptive purpose was to offer procedural protections to those engaged in public communication.[148] Implicit in the Act's prohibition of searches and seizures is the assumption that a search—even with a warrant's probable cause requirement—was inferior to a *subpoena duces tecum* to protect the interests that the drafters of the statute had in mind.[149] Specifically, there was concern in Congress that the use of a warrant would allow the government to invade nonsuspects' privacy where voluntary compliance or a subpoena would also work and be less intrusive.[150] Moreover, a newspaper's ability to publish pending stories and attract confidential sources to help inform the public in part depended on an operational continuity that would survive interaction with law enforcement.

With this history in mind, the potential protected interests can be sorted into protections for the person in possession of the materials or for a third party to whom the materials relate whose privacy might also be implicated in a search or seizure. Furthermore, the potential interests can be classified as relating to categorical interests in speech, privacy, or anonymity, as well as an interest in the operational continuity in investment-backed information-dissemination operations.

One can identify more than one discrete relevant interest in the category of privacy. A blogger might wish to remain anonymous or write

---

[145] *See id.*

[146] One commentator suggests a "clear statement" rule; "[i]n other words, unless Congress expressly states in a statute that it intends to impose procedures on state and local governments, courts should not read such implications into an act." *See* Sillin, *supra* note 123, at 440 (considering whether the Act mandated certain warrant procedures for state law enforcement officials). It would be unusual for a clear statement rule to apply to a mere determination of the purpose, object, or policy of the Act or an inquiry into its protected interest.

[147] *Cf.* SEC v. C. M. Joiner Leasing Corp., 320 U.S. 344, 350–51 (1943) (noting that courts will construe an act in conformity with its purpose and policy).

[148] *Cf.* Sillin, *supra* note 123, at 440, 466–67 ("The dissent correctly stated that the overall purpose . . . was to statutorily raise the standards of the Fourth Amendment to protect actions of those engaged in First Amendment activities."). *But see* Work, *supra* note 140, at 230 ("[T]he true privacy interest protected in the Privacy Protection Act of 1980, *limiting newsroom searches*, is not immediately obvious." (emphasis added) (footnote omitted)).

[149] *See* S. REP. NO. 96-874, at 4 (1980) ("The Committee believes that the search warrant procedure in itself does not sufficiently protect the press and other innocent third parties and that legislation is called for.").

[150] *See id.*

under a pseudonym.[151] Work product and documentary materials involve privacy in two ways. If the Act relies on compliance with a subpoena rather than allowing law enforcement officials to search, it ensures that the "mental impressions" notated in work product are not seen by prying eyes.[152] Anonymous sources or whistleblowers are also less likely to be chilled from bringing information forward to those that may publish them if law enforcement is not allowed to rifle through it under false pretenses.[153] Potential anonymous sources find comfort in knowing their identity will not be revealed to law enforcement accidentally through a haphazard execution of a search warrant and that the recipient of a subpoena has the opportunity to challenge that subpoena in court.[154] The opportunity to respond to a request from law enforcement for information or documents, such as that which attaches to a subpoena, allows the holder of such records to attempt to prevent immediate breach of these types of privacy.

One can also identify multiple discrete relevant interests within free speech. Prohibiting a search ensures that speech is not chilled by the fear of sudden physical intrusions by law enforcement.[155] Additionally, the Act's protections are tied to the public's right to receive information.[156] This logic is especially strong if one interprets the Act to be primarily about the institutional press, as some say that the press serves a structural role in our constitutional system as an adversary to the Executive.[157] One might also

---

[151] *See* Solove, *supra* note 107, at 121, 145–46 (noting that government probing can deprive speakers of the anonymity that is key to forthright expression and citing numerous cases that have concluded that the First Amendment requires a heightened standard for an anonymous speaker's identity to be revealed).

[152] *See* S. REP. NO. 96-874, at 10 ("For example, a reporter may prepare an article which his editor decides should not be published; nonetheless, the reporter's interview notes and draft of the article would remain protected by the statute. Similarly, all of an author's research notes would be protected, although only part of the research was ultimately included in the published product.").

[153] *See* Work, *supra* note 140 ("Another interest arises from the forced release of information obtained under a promise of confidentiality, possibly leading to a drying-up of sources and a diminishing of the flow of information.").

[154] *See* Solove, *supra* note 107, at 162 ("[U]nlike with subpoenas, people cannot challenge warrants beforehand."). The extent of First Amendment protections for reporters is beyond the scope of this Note. *See generally* 2 LEE LEVINE ET AL., NEWSGATHERING AND THE LAW § 16.06 (4th ed. 2011) (discussing the lack of clarity in First Amendment privilege for reporters).

[155] *See* S. REP. NO. 96-874, at 9 ("The Department of Justice . . . sought to avoid the chilling effects of disruptive searches on the ability to obtain and publish information for all those who have a purpose to disseminate information to the public.").

[156] *See id.* at 10 ("Key to the legislation is the concept of public communication. It is this flow of information to the public which is central to the First Amendment, and which is highly vulnerable to the effects of governmental intrusiveness."); Solove, *supra* note 107, at 146–47 ("A corollary to the right to free speech is the right to receive ideas.").

[157] *See* Potter Stewart, *"Or of the Press,"* 26 HASTINGS L.J. 631, 633 (1975) ("[T]he Free Press guarantee is, in essence, a *structural* provision of the Constitution."); Work, *supra* note 140, at 230 ("The strongest interest of the news media seems to be in not being a tool of law enforcement, an objection grounded in the watchdog role of a free press that is institutionally antagonistic to, or at least skeptical of, government.").

conceive of the Act as protecting one's interest in being the first to distribute protected materials in public communication. A Justice Department attorney echoed this interest when he referred to "expressive activity in utero," summarizing the Act as protecting "things which are intended to become public" rather than private facts.[158] Lastly, the interests above feed into the interest a person in the business of publishing has in operational continuity—a major concern for app developers of whom reliable delivery of information is expected.[159] Given that the Act provides a cause of action for damages, those who suffer economic losses are in a better position to recover based on the loss of operational continuity.[160]

Solove's distinction, between those actions that indicate "belief, discourse, or relationships of a political, cultural, or religious nature" and those that do not, best protects the continuous production of public communication.[161] An app developer who hosts her own content would have a more difficult time distributing content were her server seized, whereas a typical blogger could still post from a smartphone, a public library terminal, or some alternate accommodation. The distinction, however, might protect the expression of a noncommercial blogger over an app developer who deals in minimally expressive content. Additionally, especially if container-level protection is not offered to commingled digital materials, we must determine whether the business interests of a commercial app developer who wants to continue operating in the face of law enforcement inquiry are indeed in the Act's sights.[162]

Of course, without text upon which we might hang a way to cabin the interests protected by the Act, a textual reading reaches broadly to each interest described above. Such a broad reading may be justifiable in light of the Act's First Amendment roots, but it poses very real problems for ongoing enforcement.

---

[158] Eckenwiler, *supra* note 9, at 726. At the time of the address, Eckenwiler was an attorney with the Justice Department's Computer Crime Section of the Criminal Division.

[159] *Cf.* Berkowitz, *supra* note 130, at 65 (calling the Act's protection a property right in documentary materials and work product).

[160] *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Serv., 816 F. Supp. 432, 434, 438 (W.D. Tex. 1993) (noting that during the three months without its seized equipment, Steve Jackson Games claimed a total of over $150,000 in out-of-pocket expenses, lost sales, and lost profits and awarding $8781 in expenses and $42,259 in compensatory damages), *aff'd*, 36 F.3d 457 (5th Cir. 1994).

[161] *See* Solove, *supra* note 107, at 153.

[162] Much of the practical difference rests on whether the information provider hosts its own content or not. It might thus be helpful to conceive of our archetypes as the do-it-yourself or commercial server operator as opposed to a person reliant on cloud technology for continuity. Of course, this view of the information industry also needs to take into account the interest in operational continuity that a cloud service provider has for its digital materials.

E. Problems with a Broad Reading of the Act

Unsurprisingly, a textual reading of a privacy statute enacted in 1980 carries multiple problems for enforcing the statute today. A broad reading of the Act could problematically interfere with state and local law enforcement's ability to tailor how searches and seizures are accomplished jurisdiction by jurisdiction.[163] This concern ultimately proves too much. The Privacy Protection Act is a quasi-constitutional "'federal-first' regulatory response[]," [164] one of many analogous federal statutes defining the government's ability to seize information from members of the public. As such, the Act is better characterized as showing the "importance of federal leadership in information privacy problems."[165]

A primary problem with such a broad reading of the Act comes down to day-to-day practicality. A textual reading of the Act introduces the potential problem of interfering with law enforcement officials' ability to ever permissibly search a computer that is connected to the Internet. Indeed, "[a]lmost every search or seizure could be understood to have some dimension that might involve a First Amendment activity because all human interaction involves communication and association. In the end, the First Amendment could swallow up all of criminal procedure."[166] The Sixth Circuit seems to have had this issue in mind in *Guest* when developing its commingling rule to lessen protection for digital files.[167] Solove's notion of protecting information where First Amendment values are implicated might be an aid in drawing a principled line, though it is not necessarily very limiting.[168] For instance, the blogger would certainly fall under the protections of the Act because personal discourse surely implicates First Amendment values.[169] The First Amendment values of the audience of the app developer would also be at issue, if not the app developer's own interests in commercial activity and speech. "[T]his flow of information to the public . . . is central to the First Amendment, and . . . is highly vulnerable to the effects of governmental intrusiveness."[170] Indeed, "[a] corollary to the right to free speech is the right to receive ideas."[171]

Without a broad reading of the Act or revision of the Act, more jurisdictions could follow the lead of the Sixth Circuit and construe the

---

[163] *Cf.* Schwartz, *supra* note 2, at 932 (expressing concern that federal preemption of privacy law would block state sectoral experimentation).

[164] Bellia, *supra* note 2, at 880, 882 (citing the Privacy Protection Act).

[165] *Id.* at 882.

[166] Solove, *supra* note 107, at 152 (footnote omitted).

[167] *See* Guest v. Leis, 255 F.3d 325, 342 (6th Cir. 2001).

[168] Solove, *supra* note 107, at 153.

[169] Note too that if a blogger were the actual suspect of a crime (and not a crime exempted under the Act), the Act would not offer protection. *See* 42 U.S.C. § 2000aa(a)(1) (2006).

[170] S. REP. NO. 96-874, at 10 (1980).

[171] Solove, *supra* note 107, at 146–47.

statute in ways that eliminate its protections in the digital realm. Alternative methods might be used to protect First Amendment actors from the sudden intrusion of a search or seizure. Given the immense challenge in updating the many out-of-date federal privacy statutes, these alternative methods may be the best route toward shielding the various protected interests we might associate with the Act. The next Part proposes both state and federal options for such alternative methods of providing protection.

IV. ALTERNATIVE MECHANISMS TO PROTECT PRIVACY AND PUBLISHERS' OPERATIONAL CONTINUITY

Should the Act indeed only represent a "vicarious concern" for the privacy and speech interests of an app developer's audience,[172] a compelling interest requirement for search and seizure in certain situations would better protect the audience's interests.[173] Additionally, pending federal privacy reform[174] may provide an opportunity to integrate the Act with other federal privacy law governing compelled disclosure and clarify the interests protected. A compelling interest requirement and stringent ex ante requirement would protect both privacy and the operational continuity of someone in the practice of information dissemination.

A. Compelling Interest Requirements

Imposing a requirement that the government have a compelling interest to access information offers a check on officials' motivations for demanding materials that implicate protected privacy and speech. Often these compelling interest requirements originate in state law. For example, Colorado's constitution underlies the standard laid out in *Tattered Cover, Inc. v. City of Thornton*.[175] There, the Colorado Supreme Court held that the state constitutional provision protecting freedom of speech protected the

---

[172] *See* Work, *supra* note 140.

[173] *See, e.g.*, Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002) (requiring a heightened showing before law enforcement could demand the purchase records of a bookseller).

[174] *See, e.g.*, *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010); Alex Howard, *ECPA Reform: Why Digital Due Process Matters*, O'REILLY RADAR (Sept. 23, 2010), http://radar.oreilly.com/2010/09/ecpa-reform-why-digital-due-pr.html.

[175] *See* 44 P.3d at 1047; COLO. CONST. art. II, § 10 ("[N]o law shall be passed impairing the freedom of speech; . . . every person shall be free to speak, write or publish whatever he will on any subject, being responsible for all abuse of that liberty . . . ."). If not for the ruling in *Zurcher*, the First Amendment of the United States Constitution could conceivably be the basis of similar protections. *See* U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech . . . ."); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) ("[The First Amendment] has broad scope . . . [and] embraces the right to distribute literature and necessarily protects the right to receive it." (citation omitted)).

circulation of books, as well as the right to speak freely.[176] The court imposed a two-prong balancing test to govern government inquiries into the book-buying habits of the public. First, the government must have a compelling need for the desired information.[177] Second, the court must balance the law enforcement officials' need for the information against the constitutional harms; motivations related to a book's contents are disfavored as implicating greater harm to free expression.[178]

Similarly, a California state statute requires notice, an opportunity to respond, and a compelling government interest whenever law enforcement officials seek to compel disclosure of user records from commercial book services.[179] This protection does not apply to voluntary disclosure of such records or when exigent circumstances exist. The California requirement combines the procedural protections of the Privacy Protection Act—prohibiting a break-down-the-door surprise search—with the more substantive protections of a compelling interest requirement to guard readers' interests.[180]

Another category of compelling interest requirements originates in federal law. Solove points to multiple lower federal court holdings that a compelling interest is necessary to support a subpoena for expressive records,[181] such as inquiring whether a customer purchased a graphically sexual novel[182] or a publication on evading taxes.[183] These decisions could form the basis of a stronger federal protection for reader or end-user

---

[176] *See Tattered Cover*, 44 P.3d at 1051 (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 64 n.6 (1963)).

[177] *See id.* at 1057. Courts are to analyze whether the information may be obtained in another way. *Id.* at 1059.

[178] *Id.* at 1059.

[179] *See* Reader Privacy Act of 2011, CAL. CIV. CODE § 1798.90(c) (West Supp. 2013). Commercial book services include bookstores as well as digital services such as Google Books or Amazon.com. *See* SB 602 (Yee) Reader Privacy Act of 2011: Updating California Book Privacy Law, ACLU of N. Cal., *available at* http://www.aclunc.org/issues/technology/asset_upload_file991_9996.pdf.

[180] *See* Press Release, Elec. Frontier Found., California's Reader Privacy Act Signed into Law (Oct. 3, 2011), *available at* https://www.eff.org/press/archives/2011/10/03 (quoting California State Senator Leland Yee: "Individuals should be free to buy books without fear of government intrusion and witch hunts. If law enforcement has reason to suspect wrongdoing, they should obtain a court order for such information.").

[181] *See* Solove, *supra* note 107, at 147 & n.196 (citing *In re* Grand Jury Subpoenas Duces Tecum, 78 F.3d 1307, 1312 (8th Cir. 1996); A Grand Jury Witness v. United States (*In re* Grand Jury Proceedings), 776 F.2d 1099, 1102–03 (2d Cir. 1985); Grandbouche v. United States (*In re* Grand Subpoena to First Nat'l Bank), 701 F.2d 115, 119 (10th Cir. 1983)).

[182] *See In re* Grand Jury Subpoena to Kramerbooks & Afterwords Inc., 26 Media L. Rep. (BNA) 1599, 1601 (D.D.C. 1998) (applying strict scrutiny to Independent Prosecutor Kenneth Starr's request regarding Monica Lewinsky's book purchase records).

[183] *See In re* Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 573 (W.D. Wis. 2007) (allowing the government to access only the records of individuals who voluntarily chose to provide their information).

privacy if made uniform nationwide.[184] These decisions model how the Privacy Protection Act might be supplemented with clearer substantive protections for those who do not possess materials being sought by law enforcement officers.

B. Federal Statutory Privacy Reform

Proposed changes to the federal privacy legislative scheme also create an opportunity for the Act's ambiguities to inform federal privacy reform. While a thorough discussion of the movement to reform federal privacy law is broader than the scope of this Note, it is useful to briefly consider updates to the Electronic Communications Privacy Act (ECPA) as a relevant example.[185] Enacted as a forward-looking statute in 1986, ECPA specifies standards for law enforcement officials to access electronic communications and data, such as in stored communications and via wiretaps, pen registers, and trap and trace devices.[186] Parts of ECPA govern law enforcement access to stored documents. Multiple organizations are campaigning to update ECPA to require a warrant to access personal information.[187]

Given the ambiguity of what materials are protected by the Privacy Protection Act, coordinated reform of the Act alongside the more frequently debated ECPA framework could harmonize the two. Debate about ECPA reform has been a locus for advocacy for unification of federal privacy law governing digital materials. Magistrate Judge Stephen Smith, troubled by the lack of appellate review resulting from ECPA's regime of gag orders and sealed dockets, advocates for reform of the "structural aspects" of ECPA.[188] Specifically, he recommends (1) notifying targets of searches and affected individuals such as "affected customers" and "subscribers," (2) "opening court files to the public," and (3) "gathering better surveillance data for Congress."[189]

While the Privacy Protection Act does not govern the same electronic materials that ECPA does, Judge Smith's focus on structural aspects of ECPA underscores the importance of the no-search rule imposed by the Act. He focuses on the need for appellate review of ECPA surveillance

---

[184] *See* Eric Robertston, Comment, *A Fundamental Right to Read: Reader Privacy Protections in the U.S. Constitution*, 82 U. COLO. L. REV. 307, 329 (2011).

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

[186] 18 U.S.C. §§ 2511–2513 (2006); *see also About the Issue*, DIGITAL DUE PROCESS, http://digitaldueprocess.org (last visited May 25, 2013).

[187] *See, e.g.*, Leslie Harris, *Not Without a Warrant*, HUFFINGTON POST (Sept. 27, 2011, 4:58 PM), http://www.huffingtonpost.com/leslie-harris/online-privacy_b_983253.html; NOT WITHOUT A WARRANT, *supra* note 3.

[188] Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 314, 331 (2012).

[189] *Id.* at 332–34.

orders. In the context of the Privacy Protection Act, the structural features of notice and opportunity to respond provide for judicial process that oversees the government's behavior. They also function as a mechanism to stop the government prior to shutting down ancillary services that would be collateral damage in an overbroad break-down-the-door search and seizure.

Not everyone agrees that notice is a proper solution. At least in the surveillance context, Professor Orin Kerr thinks that remedies provide a "better lever of statutory reform" than notice.[190] He argues that a statutory suppression remedy would leave targets of an investigation with a solution akin to that available under the Fourth Amendment.[191] Whatever its merits in the surveillance space, Kerr's argument cannot be successfully exported to the context of the Privacy Protection Act. It does not go far enough to protect the operational continuity interest one has when one's own public communication depends on continuous operation of servers, computers, or other infrastructure that might be seized in violation of the Act. In fact, it does not extend to nonsuspect third parties at all. The tension between the ability to continue to publish and the Sixth Circuit's commingling rule warrants a structural solution that reinforces rather than weakens the Act's structural protections.

CONCLUSION

Unsurprisingly, the Privacy Protection Act of 1980 failed to anticipate our technological present. Its ambiguities with regard to protected parties, materials, and interests are disappointing given its original lofty goals of protecting First Amendment activities and inchoate public communication. Nevertheless, a textual reading of the statute affords expansive protections to people who communicate information to the public, though it seems that this broad protection remains unrealized in today's enforcement context. While the text literally bears this interpretation, this reading raises concerns about the Act's practical viability. And, while a *subpoena duces tecum* is impliedly the Act's preferred mechanism, it does not protect the privacy of those not in possession of materials sought.

In light of these weaknesses, two avenues may strengthen, clarify, and update the Act's protections. A consistent federal compelling interest standard would clarify the interests protected by the Act (those of the possessor) and the First Amendment subpoena standard (those whose information may be held by the possessor). Furthermore, reinforcement of the Act's no-search rule in federal privacy reform could help the federal

---

[190] Orin Kerr, *Notice and Opportunity to Challenge Evidence Collection Under the Electronic Communications Privacy Act: What's the Best Rule?*, VOLOKH CONSPIRACY (July 24, 2012, 2:52 AM), http://www.volokh.com/2012/07/24/should-ex-ante-court-order-requirements-also-come-with-notice-requirements-and-if-so-when.

[191] *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 807–08 (2003).

privacy legislative scheme more clearly address both substantive protections (through the probable cause warrant standard) as well as procedural protections (through the prohibition on sudden searches and seizures). The slogan "not without a warrant"[192] may be satisfyingly succinct, but one might imagine adding "and only if it is worth it" to help federal criminal procedure effect a unified federal privacy scheme.

[192] *See* NOT WITHOUT A WARRANT, *supra* note 3.