Band-Aid on a Bullet Wound: Why the Email Privacy Act Is Necessary Triage in Federal Technology Law

Bridget Dempsey

Follow this and additional works at: https://via.library.depaul.edu/jatip

Recommended Citation
Available at: https://via.library.depaul.edu/jatip/vol24/iss2/4
BAND-AID ON A BULLET WOUND:

WHY THE EMAIL PRIVACY ACT IS NECESSARY
TRIAGE IN FEDERAL TECHNOLOGY LAW

I. INTRODUCTION

People check their email everywhere these days: on the train, in class, during the morning drive, while waiting in line, and at half time. Doing this with so many people around, it is likely someone else who has not bothered pulling their own phone out is reading over your shoulder. So there is not really any reasonable expectation of privacy, is there? But what about those messages you save to read when you have a quiet moment and are not surrounded by inquisitive eyes – those messages must just be between you and the sender… right? Wrong. Privacy concerns have been making headlines, but reading about the subject leads to unfamiliar technical acronyms and shows just how little most of us really understand about the network mechanics that power the Information Age. The problem with Internet privacy though is not really consumer understanding, it is outdated legislation applied inconsistently by the courts.

Passed in 1986, the Electronic Communications Privacy Act ("ECPA") currently governs Internet privacy and is meant to criminalize unauthorized access of electric communications.1 Its subset, the Stored Communications Act ("SCA"), addresses when and how an Internet service provider ("ISP") may make voluntary or compelled disclosure of a user’s electronic communications and related records.2 The ECPA has been amended in 19943 and 2001,4 but these changes have not caught it up to the privacy expectations society has developed as America has moved online. How many hoops a government agency has to jump through in

3. Amended by the Communications Assistance to Law Enforcement Act, 47 U.S.C. §§ 1001-10.
order for an ISP to disclose content varies based on the type of information the agency wants and on whether the ISP is providing “electronic communications systems” or “remote computer services.” The result is very few hoops indeed: any agency can access an individual’s opened messages and those older than six months by its own authority if Congress granted it the power to issue administrative subpoenas.

While law enforcement’s easy means of access may come as a surprise to many, the sense of affront and zeal to reform these low requirements have been around for years and proponents of change have been gaining support and publicity. Bills to amend the SCA so that email access of any sort requires an actual warrant have been sponsored in previous Congresses, but have died before making it to the Oval Office. Now, the Email Privacy Act (“H.R. 1852” or the “Bill”) is taking up the mantle of adjusting the law to meet reasonable and widespread expectations by proposing a uniform approach to agency content seeking.

This article advocates passage of H.R. 1852 because of the sheer necessity that the current electronic communication privacy laws be better suited to the real world, while also acknowledging that the Bill’s changes are minimal in the face of the vast issues raised by the explosive proliferation of technology and the Cloud. Part II will give an overview of America’s quilt work approach to privacy law and examine the approach to communication in particular. Part III will explore the current state of the privacy issue: empirical data about American use of the Internet and email, recent case law, the failure of bills similar to H.R. 1852, and the state law response. Part IV will analyze the Email Privacy Act itself, including the changes it plans to implement. Part V will weigh the merits and drawbacks of the arguments for and against H.R. 1852, show why it should be adopted, and consider other issues left outstanding because of the Bill’s limits.

II. U.S. PRIVACY LAWS

A. The Big Picture

Americans tend to feel very strongly about their privacy and many assume it is included in their guaranteed constitutional rights, yet “privacy” does not appear even once in that seminal document. It was not until the 1965 case of Griswold v. Connecticut that the Supreme Court recognized a penumbral protected right of privacy. And even then, the Court was shielding privacy in decisions, not information. Later court decisions followed suit, but information privacy received little attention. Instead, information was protected by a variety of specialized laws addressing the use of privacy in specific contexts (health care, finance, communications, and education) as such security became necessary. The smattering of state and federal laws has evolved into a nightmare allowing lawyers specializing in even one complex sector to be highly valued. Despite being a very important area of law, it is exceedingly inaccessible thanks to the context-specific approach and the dense, complex style of many of the implementing statutes.

People’s expectations about privacy fall more in line with the Fourth Amendment, which prohibits “unreasonable searches and seizures” without probable cause and a warrant. But while the language in the Constitution may seem short and sweet, courts

12. ECPA, see note 1.
14. U.S. CONST. amend. IV
have clashed in determining when a warrant is required. For a few decades, the courts followed the decision in *Olmstead v. United States* in which the Supreme Court limited the protective applications of the Fourth Amendment by requiring physical trespass in order to find a search or seizure that requires a warrant.\textsuperscript{15} *Olmstead* and similar holdings were overruled in 1967 with *Katz v. United States* when the Supreme Court majority determined that the protection of the Fourth Amendment applies to people, not places; physical trespass on property was no longer the guiding principle.\textsuperscript{16} Justice Harlan's concurring opinion articulated the accepted two part test to determine whether an individual could reasonably expect constitutional protection of privacy: the individual actually expected privacy (subjective) and society considers it reasonable for the individual to expect privacy in such a situation (objective).\textsuperscript{17}

Despite the tremendous change *Katz* brought to privacy law, bigger technological changes would soon reveal the holding's shortcomings. By the 1980s, it became apparent that privacy expectations were not black and white. The federal courts decided that warrants were not required when the potentially invasive technology was serving merely to enhance a physical sense, but would be required if the information the technology was gathering would not otherwise have been available without a warrant.\textsuperscript{18} State courts tended to take a narrower reading of the Constitution and gave privacy protection more broadly.\textsuperscript{19} The matter came again


\textsuperscript{17} Id. at 361 (Harlan, J., concurring).

\textsuperscript{18} Compare *United States v. Knotts*, 460 U.S. 276 (1983) (holding that science and technology that augment inherent physical senses do not amount to searching or seizing and their use thus do not require a warrant) \textit{with} *United States v. Karo*, 468 U.S. 705 (1984) (holding that the use of science and technology that give information the government wants but otherwise would not be able to attain without a warrant amounts to a search or seizure sufficient to trigger the protection of the Fourth amendment).

before the Supreme Court in 2011 in *United States v. Jones*, wherein the majority revived trespass on private property as a form of search or seizure necessitating a warrant.\(^{20}\) The Court reasoned that *Katz* and Justice Harlan’s test co-existed with the older trespass rule.\(^{21}\) But even this joining of Fourth Amendment rules does little to make them more applicable to modern issues.

Thanks to the application of the third party doctrine, whereby an individual disclosing private information to any third party has lost the reasonable expectation that such information remains private, the government faces few obstacles in any endeavor to access the myriad data used via Internet connection.\(^{22}\) The inability of privacy laws to adequately translate to Internet issues illustrates a significant flaw with current privacy law. There is a growing belief among legal scholars that privacy should no longer be the focal point of Fourth Amendment inquiry, because it is becoming a quaint concept of the past and that instead this provision of the Constitution should focus on preventing undue government power to intrude.\(^{23}\)

**B. Communication**

Since the Court’s expansion of privacy expectations, communication privacy has been the most difficult to regulate. By liberating an individual’s right to freedom from search or seizure from physical trespass,\(^{24}\) *Katz v. United States* prompted legislative response. The Supreme Court decided that listening to and recording conversations in which the parties believed theirs were


\(^{21}\) Id at 947.

\(^{22}\) Pan, supra note 16 at 1024.

\(^{23}\) Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L. J. 1309, 1311-12 (2012). Ohm believes that given technological developments the country is moving toward a surveillance society. He thinks it is inevitable that the government will have a system that invades privacy which is a regularly used law enforcement mechanism – expectations of privacy will no longer be applicable as this reality emerges. Therefore, instead of focusing on privacy, Fourth Amendment application should focus on whether the exercise of this surveillance power is proportionate to the anticipated crime(s).

the only ears present amounted to a "search" and required the same sort of procedural requirements as any other: probable cause and a warrant. In light of this decision Congress passed the Wiretap Act one year later. Part of the Omnibus Crime Control and Safe Streets Act, the Wiretap Act reflected the legislature's interpretation of reasonable expectations of privacy and made electronic surveillance a legally permissible form of search so long as it was conducted with the permission of the courts.

The Wiretap Act was sufficient for a while, but the nation was on the precipice of monumental change by the 1980s as wireless phones, computers, and email were beginning to saturate the market. It became apparent that new laws were needed to continue to protect the reasonable expectations of privacy in communication first judicially recognized in 1967 with Katz. Attempting to set a framework that would be effective for years to come, Congress passed the Electronic Communications Privacy Act in 1986. In a subset of the ECPA, the Stored Communications Act, email was recognized as a unique form of communication, but the privacy protection it received would be dependent on reasonable expectations based on which type of Internet service provider was hosting the message.

1. Acronyms within the SCA: ECS and RCS

The SCA designated two possible types of service an ISP could provide. An "electronic communication service" ("ECS") is any service providing the ability for a user to send or receive electronic communication. It is meant to protect communications during

25. Id. at 353.
27. Id.
their time when used to actually convey information. It also includes “electronic storage,” which encompasses content that was backed up by the ISP in order to ensure messages were properly sent, delivered, and received. A “remote computing service” (“RCS”) is any service providing computer storage or processing services. It intends to protect communications that were storing or processing information for the user.

This distinction made sense at the time because ISPs did not provide limitless storage. Emails were generally stored as ECS for three months before being automatically deleted. Users knew that was the amount of time they had to access their messages this way, so it was during that time period that emails were part of “communication” and thus entitled to heightened privacy protections. The timeframe for privacy under an ECS was extended to 180 days in the SCA, roughly twice the amount of time users would reasonably expect to access their messages.

Content still existing after 180 days was considered stored indefinitely by the user and because it had been left in such a state, was deemed less secure, less susceptible to reasonable expectations of privacy, and therefore more readily accessible for search.

2. What Is Necessary to Search Electronic Content?

The significance of this distinction was to tailor pre-search efforts to the public’s reasonable electronic privacy expectations. Unread ECS mail, still in electronic storage for less than six months, could be expected to be accessed and used privately – thus these sorts of messages require the strictest mechanisms to compel disclosure: a judicial search warrant issued in response to probable cause. Unread RCS mail unaccessed for more than six months

32. Id.
34. Mulligan, supra note 28 at 1568.
36. Id.
was effectively abandoned on the ISP’s servers and accordingly was not entitled to high expectations of privacy – an agency needs a subpoena, which it may be able to issue itself, and to give the user notice that it was conducting a search.  

37 Mail that a user opened has effectively completed the live “communication” aspect of access and is not in electronic storage because the ISP has discharged its function of enabling communication and is not storing for those purposes. Thus the user has effectively abandoned the message and cannot support a reasonable expectation of privacy; the agency needs only a subpoena.  

38 The variety of authorization and notice these permutations require for disclosure reveal the importance of the ECS/RCS distinction.

III. SETTING THE STAGE

But it is silly for two acronyms that are so unknown to the public to be so important on a regular basis in Internet communication. The world is moving online. As the country increasingly turns to the web for everything from makeup tutorials to medical treatment, the laws protecting (or not) the communication that takes place there should make changes too. Instead, judges who took classes on the law, not computer engineering, are struggling to force Athena back into Zeus’ head, but with little success. Congress has noticed and introduced bills similar to the Email Privacy Act in the past, but they have not been able to go the distance. And while the national government has floundered, states have started taking action on their own. The Eighties are most definitely over.

A. American Internet Usage

The importance of the acronym attached to a message is obvious, but determining which acronym fits is enigmatic. Digital developments and the rise of the Cloud have made gigabytes of storage available for free. Such a quantity was unfathomable in 1986. A Pew study of Internet use over the last twelve years

shows that only 46% of Americans used the Internet in March of 2000; by August of 2012, that number rose to 85%. Of those who did use the Internet during that same span, the number using email nearly consistently remained above 90%. None of the other uses inquired about showed even close to this wide prevalence.

B. Judicial Troubles Applying a "__CS" Label

During that same period the country was rapidly adopting the Internet and email, disputes were arising that forced the courts to make rulings based on the highly technical and no longer relevant distinctions of early Internet Service Providers ("ISPs"). The result was a circuit split incomprehensible to the average AOL user. Reading the Stored Communications Act can be confusing in and of itself, but trying to figure out how that law actually applies – and who is the appropriate body to decide that is further baffling.

Online information privacy is supposedly regulated by the Federal Trade Commission ("FTC"), but the sheer variety and quantity of virtual data led the agency to limit its own jurisdiction and adjudicate only a small number of violations. The FTC focuses on holding companies accountable to their self-published privacy policies; little or no effort is given to preventing fellow government agencies or private citizens from broadly digging through what the public perceives as private information. Instead those invasions are left for individuals to protest themselves and thus are usually only protested when they produce evidence.
against an individual in some civil or criminal suit. The agency’s reluctance to take on the hydra of digital privacy is understandable though when considered in light of the struggles courts have faced in applying the SCA.

California 2003: The Ninth Circuit addressed whether a lawyer’s use of an abusively broad subpoena for stored email from an ISP violated federal electronic privacy and computer fraud statutes. Starting from an approach interpreting the SCA in light of common law trespass, the Court found that the lawyer had acted outside the law. It then dove into an analysis of “electronic storage.” Focusing on the use of “backup” in SCA § 2701(B), the court focused on whether messages stored potentially indefinitely could still be considered ECS. The court held was that they could because the storage was still for the sake of messaging at the convenience of the user. The implication of the court’s holding was that old messages not deleted were in no way abandoned and the user maintained a reasonable expectation of privacy.

Four years later, the Ninth Circuit further bolstered its stance that the age of a message did not make it fair game for law enforcement officials with its holding in United States v. Forrester, in which the court ruled that privacy interests in email are identical to privacy interests in postal mail. It made another consistent ruling in Quon v. Arch Wireless Operating Co., Inc. but this string of cases would be called into question when the Quon case made its way to the Supreme Court.

In making its decision in Quon, the Supreme Court avoided analyzing the application of the Fourth Amendment to digital messages and instead issued a narrow holding focused on whether the search of an employee’s text messages on an employer-

44. Id.
45. Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003).
46. Id. at 1072-74.
47. Id. at 1076.
48. Id. at 1077.
49. Id. at 1075-77.
50. See generally United States v. Forrester, 512 F.3d 500 (9th Cir. 2007).
provided pager, considered an invasion of privacy by the user, was reasonable. Taking many of the issues the Ninth Circuit had considered in detail, especially the implications of the ECS/RCS distinction, arguendo and not offering any opinion on them, the Supreme Court avoided the technical tangle concerning civil liberties. Instead it played up employer supervision of employees for business purposes. The result provided little insight in how courts should address searches under the SCA.

Six months after the Supreme Court decision was released, the Sixth Circuit focused on privacy expectations in the reasonableness of searches involving email in United States v. Warshak. In a controversial decision, the Warshak court also ignored the ECS/RCS issue but instead followed Forrester in equating email, no matter its age, to postal mail and requiring a warrant for search. The opinion gave an extensive summary of its reasoning focusing on the important role email plays in today's society and how it is eclipsing traditional communication methods of telephone calls and postal mail.

While many courts sidestepped the label issue, in 2012, the Supreme Court of South Carolina directly addressed the ECS/RCS distinction, focusing on the "backup" provision just as the Ninth Circuit had. However, in a confusing plurality opinion, which highlighted how opaque the SCA is, the court took the opposite stance of the Ninth Circuit and held that old, opened emails were not ECS and thus were entitled to less protection. All five Justices agreed on the holding but reached it by three different sets of reasoning. Two Justices focused on the fact that the old messages only existed on the ISP's servers and therefore could not be considered a plain language "backup" feature of the messaging service because no other copies existed. Two others Justices

53. Id. at 758-59.
55. Id. at 285-86.
56. Id. at 284.
58. Id.
59. Id. at 245.
60. Id. at 243-44.
rejected this reasoning instead noting that the continued existence of the old messages on the ISP servers was a default and not for the service provider’s use in ensuring effective service; thus the existence of the messages did not fit the statutory language describing when a message is an ECS backup and only received RCS protection.61 The fifth Justice largely agreed with the statutory analysis, although not entirely.62

C. The Building Momentum for Reform

Some Congressmen paid attention to the increasing failures of the SCA to adequately address digital communication. In 2011, Senator Patrick Leahy introduced Electronic Communications Privacy Act Amendments Act of 2011.63 That bill, whose aims and language were similar to the Email Privacy Act in the House today, died in committee.64 A House version, sponsored by Representative Bob Goodlatte and thirty-four others, had more success. H.R. 2471 made it through the House and was reported on in the Senate, by Leahy, but never gained enough attention for calendar prioritization or debate.65 It too died without a vote.66

D. States Stop Waiting for the Feds to Take the Lead

While lawmakers’ reform efforts stalled out in Washington, the Texas legislature decided to take action on its own to protect citizens’ privacy in electronic communications. H.B. 2268 was introduced in the state House of Representatives in March, made it to the Senate in May, and was signed into effect by the governor in

61. Id. at 246-48.
62. Id. at 249.
June. The entire process took less than four months and Texas can now boast it has the nation’s strongest email privacy law. State law enforcement officials are required to get a warrant before any search of email content.

IV. THE EMAIL PRIVACY ACT

A. Who, Where, and When

House Representatives Kevin Yoder [R-KS] and Tom Graves [R-GA] introduced the Email Privacy Act as H.R. 1852 on May 7, 2013. It was promptly referred to the House Judiciary Committee’s subcommittee on Crime, Terrorism, Homeland Security, and Investigations, where it still remains. Within two weeks it began drawing bi-partisan support and now has 197 co-sponsors, 68 of whom are Democrats. There has been at least one new co-sponsor every month since its introduction.

B. What, Why, and How

The Email Privacy Act intends to update privacy protection for information stored by Internet service providers while balancing

69. Id. Texas’ prior law on point had mirrored the ECPA with different standards depending on whether a message had been opened and how long it had been in an inbox. Those distinctions have been eliminated.
70. Press Release, Kevin Yoder, Representative Yoder, Graves Introduce Email Privacy Act (May 8, 2013) (on file with author).
72. Id.
consumer interests with law enforcement needs. Its first section summarizes its purpose by providing its short title.\(^74\) Section two proposes to amend 18 U.S.C. § 2702(a)(3), the provision charging ISPs to protect users' information privacy from invasion, so that it is easier to read and to emphasize that ISPs should not divulge the contents of any communication or records of a customer to the government.\(^75\) The next section makes more substantial amendments. It addresses 18 U.S.C. §2703 and eliminates subsections (a), (b), and (c) and replaces them with new provisions.\(^76\)

1. Clearing Up the Law: Eliminating Distinctions Based on Age and Streamlining Notice

By removing subsection (a), the Bill effectively abolished the 180-day distinction that has been critical in determining what sort of authorization a government entity needs before it can access an individual’s email. The proposed language requires that no matter the age of an email, the government needs a court issued warrant, rather than possibly just an agency issued subpoena, to go through the files a person stores on the Web.\(^77\) Revised subsection (b) condenses and simplifies the notice procedures required when a government entity does attain private content. Notice must include a copy of the warrant, a description of the nature of the government inquiry, and an accounting of the information the entity accessed.\(^78\) Law enforcement agencies must provide such notice within ten days of receiving the information and other government entities must do so within three days; however, §2705 still provides occasion when either sort of agency may delay notice.\(^79\) The changes from new subsection (c) are mostly stylistic, serving to make the law more accessible and close any potential loopholes based on a technicality in wording.

74. H.R. 1852, 113th Cong. §1.
75. H.R. 1852, 113th Cong. §2.
76. Id. § 3(a)(1).
77. Id. § 3(a)(1)(a).
78. Id. § 3(a)(1)(b)(i), (ii).
79. Id. § 3(a)(1)(b).
Section 3, subsection (a)(2) of the Bill then proposes to add a new subsection, subsection (h), to the end of § 2703. This proposed language states that the warrant requirement in approaching ISPs for content does not limit government agencies in using administrative subpoenas to force recipients of messages to disclose information or to force an ISP to disclose content if the customer of its services is the agency itself, who acquired the ISP’s services for the professional use of its employees. Subsection (b) of the Email Privacy Act §3 makes small adjustments so that the language of 18 U.S.C. §2703(d) reads consistently with the amendments.

2. Subtler Changes: Delayed Notice

Next, the Bill proposes to change the delayed notice provisions of SCA §2705. Because a government entity would now always have to receive a warrant, it would be a standard part of the warrant application procedure for the agency to have the option to apply for delaying giving notice to the subject of the investigation. Under the Stored Communications Act, law enforcement agencies could apply for a six-month delay, while other agencies would max out at ninety days. Delay is currently always limited to ninety days, but because a warrant is not always required, it commonly lays in the hands of the agency to determine whether or not to exercise the delay. Furthermore, the government entity could apply for subsequent ninety-day delays; this extension remains, but now reflects the importance of law enforcement in allowing those agencies to apply for six-month delay extensions. When all delays and extensions have expired the Bill’s updated version of § 2705 would require that the ISP customer whose information was disclosed receive notice that

80. Id. § 3(a)(2).
81. H.R. 1852, 113th Cong. § 3(a)(2).
82. Id. § 3(b).
83. Id. § 4.
84. Id. § 4(a)(1).
85. Id. § 4(a).
includes a copy of the warrant, a description of the inquiry, an accounting of the information sought and revealed, the dates of the warrant’s issue and exercise, a disclosure of the delay, the details about which court authorized the delay, and the reasons the delay and any subsequent extensions were authorized.\textsuperscript{88}

In delaying notice, the Bill also amends § 2705(b) whereby the government agency can order the ISP to delay notice for the same periods of time and based on the same reasons that the agency itself may delay notice.\textsuperscript{89} Stylistic alterations make this portion of the Bill clearly reflect the language used earlier addressing when the agency may delay. A new subject under this topic is addressed by the addition of a subsection (4) under which the ISP would have to give notice to the government agency three business days before providing any sort of notice of the disclosure to the customer.\textsuperscript{90}

H.R. 1852 then makes sure to add a subsection (c) to 18 U.S.C. § 2705 in order to define law enforcement agency as an agency authorized by law to “engage in or supervise the prevention, detection, investigation, or prosecution of any violation of criminal law, or any other Federal or State agency conducting a criminal investigation.”\textsuperscript{91}

3. \textit{All New: Accountability}

Next, the Bill moves to address transparency concerns. In § 5 it proposes that by September 30, 2015, the Comptroller General should make a report to Congress detailing private communication disclosures and how they were acquired from 2010-2015, including providing the number of instances of such disclosures, the response times of ISPs, the number of requests of such disclosures, and the number of requests for delays of notification.\textsuperscript{92} This report should also analyze and evaluate the effects of the changes wrought by the Email Privacy Act on the courts, which

\textsuperscript{88} Id. § 4(a)(4).
\textsuperscript{89} Id. § 4(b).
\textsuperscript{90} Id. § 4(a)(4).
\textsuperscript{91} Id. § 4(c).
\textsuperscript{92} Id. § 5(1).
would now be burdened by always having to make the
determination whether to issue a warrant, as well as the response
time of ISPs in complying with such warrants or having to be
called before the court to order such compliance, and whether the
additional legal procedures had any effect on the use of the
emergency loophole in § 2702(b)(8).93

4. Some Things Stay the Same: Other Surveillance Laws

Finally, §6 of the Email Privacy Act clarifies that the changes its
earlier sections make are not intended to be read as making any
changes to other surveillance laws.94

V. H.R. 1852 Under Review

The changes proposed by the Email Privacy Act may seem like
minor adjustments that just make the law say what people already
think it says, but despite its seemingly innocuous objectives, it has
become a subject of debate not just on its merits but on how the
legislature should operate. The Bill’s champions focus on the years
that have made the law stale, the unforeseeable technological
change, and the need for the law to work with and for society.
Detractors concentrate on how H.R. 1852 does not go far enough
and that putting effort into its passage would be crippling to a real
reform effort.

A. Give It a Try: Proponents of H.R. 1852

While the Email Privacy Act has not received widespread media
coverage, most who have joined the conversation are hopeful
advocates. The courts and Congress have made certain that the
public is justified in maintaining a reasonable expectation of
privacy when talking in person, when sending letters through the

93. H.R. 1852, 113th Cong. §5(2); 18 U.S.C. §2702(b)(8) allows an ISP to
disclose information to a government entity without any subpoena or warrant if
the ISP in good faith believes there is an emergency risk of death and or serious
physical injury which justifies such a disclosure.

mail, and when making a phone call – why should messages sent over the Internet be any different?

"They should not" is the answer which is gaining momentum across the country. The email service providers themselves have long supported the change: Google, Microsoft, and AOL have voiced dissatisfaction with the Electronic Communications Privacy Act. They have banded together with other service providers and tech companies like Amazon, Facebook, IBM, and Twitter by forming an alliance, the Digital Due Process coalition to speak with a unified voice in their drive for reform. Other groups and organizations have sprung up to bring the electronic privacy message to the masses: the Center for Democracy & Technology focuses on keeping the public and policy makers informed while trying to bring together Internet companies and Congress; the Electronic Frontier Foundation's mission centers on preserving civil liberties online; TechFreedom directs its attention on a pragmatic approach to technology reform; Fight for the Future works on viral production and promotion of tech law infographics and petitions to lawmakers; and Demand Progress promotes grassroots lobbying.

These organizations advocate that technology law, specifically the ECPA, "needs to be brought in line with how people use the

---


Internet today.” As more and more economic growth and social activity takes place online, law needs to work with the web, not against it. Google has vocally supported the Sixth Circuit’s holding and reasoning in *Warshak* and taken independent action to implement a reform featured in H.R. 1852.

With so many big names talking about the issue and the increasing public awareness and support, it is little wonder that policymakers began to get involved. In a hearing before the House Judiciary Crime subcommittee, the Department of Justice admitted that the ECPA needs reform because “the lines drawn by the SCA that may have made sense in the past have failed to keep up with the development of technology, and the ways in which individuals and companies use, and increasingly rely on, electronic and stored communications.” Senate president pro tempore Patrick Leahy, who sponsored a bill that mirrors H.R. 1852, says the matter “is not a Democratic issue or a Republican issue -- it is something that is important to all Americans, regardless of political party or ideology.” A few months later, when Representative Yoder introduced the Bill in the House he noted that part of the Bill’s purpose was to give effect to “what most Americans already assume,” that their privacy is protected from government intrusion.

---


99. *Id.* Since 2010 Google has issued Transparency Reports detailing government requests for information and their compliance – if H.R. 1852 is passed, it would require the government to make such an accounting itself.


102. Press Release, Kevin Yoder, Representative Yoder, Graves Introduce Email Privacy Act (May 8, 2013) (on file with author).
H.R. 1852 would go a long way toward bringing the antiquated privacy laws related to email closer in line with the public’s expectations. Americans are very protective of their right to privacy. They know that when the concerns of society trump the concerns of the individual, like when some crime has been perpetuated, law enforcement can override those rights. The key to comfort with sacrificing individual rights is the warrant. There seems to be little way to have an absolute guarantee of privacy in any act or communication, but there is a difference between potential exposure when under investigation and unknown exposure from reconnaissance; the first may be unpleasant, but discovery of the second can leave a person feeling violated. This sort of invasion attacks an individual’s sense of security but the law allows it on occasion when the searching party can make a good showing that notice of searching and surveillance could lead to steep harms. In most instances, however, the searcher must get a warrant and give notice.

The Bill would extend warrant procedural requirements to all searches of email. Section 3 of the Email Privacy Act would simply be bringing the rules governing email, one of the most utilized forms of communication, in line with the rules governing other common methods of communication. Though the laws governing different types of communication privacy will not become uniform, the Bill’s warrant requirement for email searches will help line up this privacy expectation with other common communications methods more effectively. This mutuality of governance would make the entire subject area both more understandable and accessible to society. And on an individual level, this will align law with a person’s subjective understanding or expectations of privacy—the first of the two elements necessary


104. The ECPA lists these harms (endangering an individual’s life or safety, fleeing prosecution, spoliation of evidence, intimidation of a witness, and otherwise jeopardizing an investigation or delaying trial) as “adverse results” in §2705.

105. H.R. 1852, 113th Cong. §3; *see supra* Section IV, Part B.1
to show "reasonable expectation" for Fourth Amendment protection. 106

Not only would H.R. 1852 make communication privacy laws more cohesive, it also is a better reflection of American society’s online privacy expectations. What society would reasonably expect is the second inquiry of the test for Fourth Amendment protection. 107 By passing H.R. 1852, Congress would be making statutory law that comports with the standards of reasonable expectation of online communication privacy the courts have been building for years. The proposal and support of the Bill demonstrate that some of the legislature has recognized that the public has expressed expectations that privacy law should protect email the way it protects mail. Passage of H.R. 1852 would be a step for the government in keeping with the times and responding to the people. 108

The adoption of the Email Privacy Act would serve as a reflection of modern society, as laws are meant to do. It could also help provide the impetus for needed, related reform in other areas of technology law. By addressing fundamental liberty concerns, good cause and judicial before search or seizure, H.R. 1852 lays a necessary foundation for digital communication privacy law reform.

B. Why Bother? Opponents of H.R. 1852

Yet the ideals driving the support for the Email Privacy Act can easily be criticized. The opponents of the Bill take a somewhat more cynical but also more realistically practical look at the state

106. Warshak, 631 F.3d at 284.
107. Id. at 284-86.
108. Online articles and petitions urging the public to contact policymakers and voice their support for H.R. 1852 are numerous- especially when a blast of them appeared on February 27, 2014 – see Mark M. Jaycox Congress Must Update Email Privacy Law Electronic Frontier Foundation https://www.eff.org/deeplinks/2014/02/ congress-must-update-email-privacy-law (last visited Mar. 5, 2014) (also posted on numerous tech news sites); Mark Stanley Tell Congress to Support the Email Privacy Act Center for Democracy & Freedom https://www.cdt.org/blogs/mark-stanley/2702tell-congress-support-email-privacy-act (last visited Mar. 5, 2014).
of affairs by focusing on the difficulties with implementing the changes advocated by H.R. 1852. They are skeptical of whether the amendments will make any real difference other than creating procedural hoops and further burdening busy courthouses. ¹⁰⁹

Many of the more vocal opponents of the Bill are in fact zealous supporters of technology law. They feel that the changes in the Email Privacy Act are a step in the right direction, but are not nearly enough. ¹¹⁰ By focusing support on a half measure, attention and support will be diverted from more substantial and meaningful reform efforts. The public’s privacy expectations themselves fall short of what people should be calling for. ¹¹¹ Adding in a warrant requirement is not much of a change, it is more an adjustment to close a loophole and ensure that communication law is consistent, whether messages are sent by post or by web.

The warrant process, while sometimes considered an inconvenience by investigators, will likely not amount to a real hardship in the email search context, especially since probable cause and search limitations will likely follow patterns established by the agencies themselves in the twenty-eight years since the ECPA was enacted. Though acquiring a warrant will still be a hurdle for investigators to clear, it will remain relatively easy for the government to get broad access in appropriate circumstances to correspondence intended to remain private. ¹¹²

¹⁰⁹. S. Rep. 113-34, Part VII Additional Views (Senators Charles Grassley and Jeff Sessions acknowledging the need for ECPA review but criticizing S.607, nearly identical to H.R. 1852, because it hampers law enforcement and civil regulation agencies like the Securities and Exchange Commission (“SEC”).

¹¹⁰. See Mark Jaycox, Update to Email Privacy Law Must Go Further, Electronic Frontier Foundation https://www.eff.org/deeplinks/2013/05/update-email-privacy-law-must-go-further (last visited Apr. 8, 2014) (discussing S.607, a bill nearly identical to H.R. 1852 and commenting that “the bill should go beyond the status quo.”). Electronic Frontier Foundation was also discussed in Part V-A as an organization advocating technology reform, but some of its analysts advocate more for big changes than what could be seen as “small fixes” like H.R. 1852.

¹¹¹. Id.

¹¹². Id. (discussing how ISPs like Google, Microsoft, Yahoo!, Facebook, and Twitter already require a warrant before they allow law enforcement to
Law enforcement officials may not suffer much added day-to-day difficulty, but the effect on the bench will be quite different. Agencies tend to have large staff and can delegate work, such as having one agent pursue a warrant while another conducts interviews. Therefore, the added warrant burden under H.R. 1852 will instead fall on the judges, a much smaller group who will see an increase on their docket, as authority to ask for a warrant is far more widespread than authority to grant a warrant. This overload will have adverse ripple effects as the judiciary’s docket becomes bogged down having to hear allegations and make rulings on sufficiency of probable cause for a greater number of warrant applications by law enforcement for investigating online records than judges are accustomed to deciding. And though in most cases the warrant requirement will just be standard procedure, another box to check off in the course of an investigation, critics fear it will become a real issue in emergency situations.113

There could also be questions about just what sort of information the warrant is required for. Although H.R. 1852 obviously requires judicial approval before accessing the content in a message, just as before seeing what is inside an envelope, opponents wonder about the other data a digital message contains.114 Is an IP address of a message sender or recipient equivalent to the address or return label on an envelope? Can it be viewed without a court order? What about GPS tags? Reform is needed, but Congress should not pass a law before addressing these questions.

Opponents feel the entire effort of H.R. 1852 is further suspect because of its built-in delay option subject to agency request and renewal. Though an agency will have had to go to court to get a warrant, the subject of the investigation could go months before receiving notice. And if some overenthusiastic or unmeticulous investigator does not go through all proper channels in obtaining a

113. S. Rep. 113-34, Part VII (considering kidnapping, where time and a quick response are vital, but information to get a warrant may be scarce because the perpetrator’s identity is unknown).
114. Id.
warrant and consequently searches email in violation of the Stored Communications Act, there is no suppression remedy in the Bill to prevent such evidence from being used in court.\textsuperscript{115} This flaw in H.R. 1852 makes the Bill look just as nonsensical as the no-warrant for email searches appears now—both are common sense judicial checks to preserve liberty that are not properly addressed by lawmakers and thereby harm the public for politicians’ poor drafting.

Furthermore, as the delay provision illustrates, H.R. 1852 distinguishes between law enforcement and other agencies.\textsuperscript{116} Opponents fear that this distinction will hamper the investigative and enforcement capabilities of civil regulatory agencies like the Securities and Exchange Commission, the Food and Drug Administration, the Consumer Product Safety Commission, and the Federal Trade Commission.\textsuperscript{117} These civil agencies do not have the authority to obtain a search warrant and therefore would be totally precluded from searching email content unless given permission.\textsuperscript{118} This effect would be crippling given how much communication takes place online.

Given how long the ECPA has lasted despite the monumental changes in technology since its enactment, it is likely that whatever amendments are made to it within the next few years will also be in place for years to come. H.R. 1852’s opponents believe Congress should instead focus on changes that not only fit the technology of today, but will be more readily adoptable to the technology of tomorrow. They feel that focusing time and efforts on this Bill is a waste when it too would have to be taken down soon as more meaningful reforms are ushered in. Small adjustments like this look helpful, but in actuality will only elongate the delay before more substantial laws replace the old framework in order to properly address the needs of today and tomorrow. This sort of alteration may even cause more harm to the reform process not just in the drain on time and resources, but also by possibly clouding the issue. The problem might be in

\textsuperscript{115} Jaycox, supra note 110.
\textsuperscript{116} See supra Part IV-B.
\textsuperscript{117} S. Rep. 113-34, Part VII.
\textsuperscript{118} Id.
place now, but the focus should still be on the bigger picture. H.R. 1852 delays the inevitable, throws good money after bad, and hurts more than it helps.

VI. Conclusion

In light of the arguments on both sides, the Email Privacy Act should be adopted. Change is needed. Now. Even the Department of Justice, this nation’s prosecutors who should be eager to maintain any means of attaining evidence to win convictions agree that the law as it currently exists is nonsensical and needs reform. Society and technology have changed radically and for the current legal system to work when applied to these new technologies, reform has to start somewhere. The changes the Email Privacy Act makes may not be as sweeping as necessary, but change does not have to come all at once. Especially in light of the opposition’s accurate assessment that contemporary laws will likely last until they become relics, it may be better to implement reform slowly in order to fully consider any recognized implications of changes and try to anticipate the effect they could have in the future, as well as to consider and adapt to new technologies.

New software is being developed far faster than the lawmaking process can keep pace with. Given the very nature of the related processes for creating code where the inspiration of a new idea or manipulation of algorithms can create a new product overnight versus drafting, presenting, rewriting, debating, and eventually passing laws of the legislative process, it is impossible to expect Washington to be constantly tweaking laws as developers create new technology. This would make law enforcement run in circles as they try to keep up with staying legal while also confusing the public and undermining the notice requirement of laws. But while the law cannot be so fluid, Congress now has the opportunity to draft with new knowledge and take up the challenge of analyzing technology and related legal implications to predict possible future issues and thus make laws over the next couple years that would be more effectively adaptable to technologies we can only guess about today. However, before legislatures take on the monumental
project of planning for the future, something needs to be done for today and the Email Privacy Act serves that function.

Concerns about judicial overload almost always arise when there are proposed changes in the standards of the law. It is a real problem, but may not be such a concern in the instant case. Consultation with and approval of a judge is already necessary for non-digital searches, adding warrants for emails should not be tremendously smothering. Instead, it may check agency investigations by ensuring that law enforcement resources are only being expended if the investigator can sign an affidavit for the court attesting to probable cause to justify a particularized data search.

Any delay in notification also requires judicial permission. The postponing of notice is not a feature being added by H.R. 1852, it is already a part of the SCA and for a rational basis.119 Being alerted to an on-going investigation could compromise many cases before they truly begin. With a judge serving as gatekeeper, it is only in cases where there is risk of physical harm, flight, spoliation of evidence, witness intimidation, or other compromise that delay is granted. Such dangers will certainly not be present in all cases of agency investigation. Furthermore, the limit on delay reflects the gravity of the matter at hand: law enforcement agencies, those officers investigating criminals most likely to pose a risk, will have the option for a longer delay; all other agencies will be bound by the same delay constraints as already exist. And again, any extensions require court approval.

It is also the judge who decides whether evidence is admissible before trial. A suppression remedy would have been an efficient touch to the Bill, but defendant’s counsel will easily be able to object to the admission of illegally obtained evidence and few judges will look kindly on the prosecutor trying to present such evidence. There are already processes in place to address this worry.

The importance of getting even a relatively small measure like H.R. 1852 passed now is exhibited by the large bipartisan support behind it. Further evidence is demonstrated by the fact that there are currently nearly identical bills titled the “ECPA Amendments

Act of 2013” in the Senate (S. 607) and the House (H.R. 1847).\textsuperscript{120} Though the Email Privacy Act has the highest number of co-sponsors, the mere presence of these identical bills shows just how pertinent the issue is. S.607 in particular has received a great deal of attention because its initial sponsor, Vermont Democrat and Senate President pro tempore Patrick Leahy, was one of the original proponents of the ECPA itself.\textsuperscript{121}

Bills with similar objectives though in different contexts of applications are also prevalent. The Reasonable Expectations of American Privacy Act ("REAP Act"), H.R. 3557, closely resembles the Email Privacy Act, although it also proposes changes to the Foreign Intelligence Surveillance Act ("FISA").\textsuperscript{122} Other bills focus on warrants and notice of government surveillance as well as government transparency in reporting the accessing of private information whether by subpoena or warrant.\textsuperscript{123} Though the 113th Congress looks like it will be the least legislatively productive body in American history, lawmakers are trying to ensure that some changes are made to better protect the people’s privacy. The Email Privacy Act is by no means the sort of history-making bill whose passage will be lauded for the ages, but it is a utilitarian proposal that can start important day-to-day changes right away while potentially paving the way for more extensive reform.

Bridget Dempsey*

\textsuperscript{120} S. 607, 113th Cong. (2013); H.R. 1847, 113th Cong. (2013).
\textsuperscript{122} H.R. 3557, 113th Cong. (2013) [REAP Act]; 50 U.S.C. §1801 et seq. [FISA].

* J.D. Candidate 2015, DePaul University College of Law; B.A. 2012, Saint Joseph’s University. Thanks to my editor and my family.