Looking Forward By Looking Backward: *United States v. Jones* Predicts Fourth Amendment Property Rights Protections in E-mail

*Jennifer Arner**

Introduction

The privacy of your e-mails depends on where you store them.[1] E-mails stored on your computer receive greater protections than e-mails stored with a third party.[2] In an age of web-based e-mail services, this distinction is easily overlooked and leads to seemingly arbitrary results.[3] For instance, should law enforcement officials who lack probable cause for a search warrant still be able to sift through your e-mails on a mere hunch that you may be conducting criminal activity? Consider a modified version of the thought experiment created by scholar, Achal Oza.

Imagine that law enforcement officials suspect two individuals, Kirk and Pamela, are taking part in a criminal conspiracy.[4] Officers believe looking through their e-mails may provide evidence of planned, coordinated crimes, but the officers lack probable cause to obtain a search warrant.[5] Is this a dead end? You may be surprised to learn that in some circumstances, the officers have the power to follow their hunch.

---

* George Mason University School of Law, J.D. Candidate, May 2014; Muhlenberg College, B.A. English & Media and Communication, May 2011. I would like to thank Professor Adam Mossoff who helped me select this Note topic, Gregory Mottla who provided me with invaluable guidance through the writing process, and Kirk R. Arner who assisted me in fact-checking and editing.

1 *See* discussion *infra* pp. 3-4.

2 *See id.*

3 *See id.*

4 This hypothetical is very closely based on Achal Oza's hypothetical in *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*. I am similarly using this hypothetical to illustrate the deficiencies in the ECPA electronic storage provision, but will instead argue for a solution of constitutional protection rather than an amendment to the ECPA. Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U. L. Rev. 1043, 1044-45 (2008).

5 *E.g.*, Oza, *supra* note 4, at 1044.

This power largely depends on the type of e-mail service used and where the messages are stored. Let us say that Kirk and Pamela subscribe to Gmail, a third-party e-mail service, and access their e-mail through a local PC-based e-mail client, Microsoft Outlook.[6] While Kirk and Pamela both have registered Gmail accounts and read their e-mails using Microsoft Outlook, they have selected different methods of delivery. Kirk reads his e-mails via the Post Office Protocol 3 (POP3) delivery standard.[7] This means that when Kirk reads his e-mails, the messages are delivered from Google's servers to Kirk's hard drive and stored within the Microsoft Outlook application files.[8] Additionally, once the e-mails are delivered to his hard drive they are no longer stored on Google's third-party server.[9] Pamela also has her e-mail messages synced to Microsoft Outlook; however, she uses Internet Message Access Protocol (IMAP)[10] delivery standard. This

---

[6] Many e-mail clients exist that handle both POP3 and IMAP e-mail standards. These are not limited to laptop or desktop computers; they also include mobile devices, such as smartphones and tablets. Outlook is just one example of a local, device-based mail client. Likewise, Gmail is but one of many third-party e-mail services, including but not limited to Yahoo! Mail, Outlook.com, and AOL Mail.

[7] POP3 stands for Post Office Protocol 3. This is what Kirk, in the hypothetical, has configured his Gmail account to use. The mail is delivered from Google's servers to Kirk's hard drive, where it is then stored within the Microsoft Outlook application files. Once this action takes place, the server's copies of the e-mails are then deleted. All e-mails are therefore read and stored on that computer. He cannot access these emails from another device. They exist solely on his hard-drive and are fully protected by the Fourth Amendment. No one can be compelled to turn over these e-mails to law enforcement without a warrant. For a more detailed explanation see Oza, *supra* note 4, at 1052; Rob Pegoraro, *Internet Providers Should Find Their Way to IMAP*, WASH. POST, March 21, 2004, http://www.washingtonpost.com/wp-dyn/articles/A10089-2004Mar20.html.

[8] *See* Oza, *supra* note 4, at 1052; Pegoraro, *supra* note 7.

[9] *See* Oza, *supra* note 4, at 1052-53; Pegoraro, *supra* note 7.

[10] IMAP stands for Internet Message Access Protocol. Pamela, in our hypothetical, also uses Gmail but has her email messages synced to Microsoft Outlook via the IMAP standard. In contrast to Kirk's email, Google's server is the primary storage location for her e-mails. Because Pamela uses the IMAP standard, her messages are being synced between Google's servers and her Outlook program instead of merely being transferred to her computer. Even if they are delivered to her computer locally, they remain on Google's servers. This is not only convenient and user friendly, but the default setting for most web-based service providers. In fact, the only difference from Pamela's point of view is that Outlook operates better using IMAP because it allows her to view identical e-mails on multiple devices. *See* Pegoraro, *supra* note 7; *see, e.g.*, Oza, *supra* note 4, at 1053.

Though the individuals in this example use Microsoft Outlook to read their e-mails, it is common for many individuals to subscribe solely to a web-based e-mail service and access their accounts through their web browser. Though web-based e-mail servers like Gmail offer the option of POP or IMAP, IMAP is predominantly the default setting, and admittedly many users do not know the difference. This means that the messages are solely stored on the third-party

means that her messages are being synced between Google's servers and her Outlook program instead of merely being transferred to her computer's hard drive.[11] Unlike Kirk's messages, Pamela's remain on Google's servers even after they are delivered to her computer locally. Though they may be receiving and reading the same messages, Kirk's messages are stored on his personal property while Pamela's are stored on a third-party server in addition to retaining a local copy within her Microsoft Outlook Application files.[12]

This distinction is significant when it comes to Fourth Amendment protections.[13] Because Kirk's messages are stored on his personal property, they are fully protected by the Fourth Amendment and will remain private so long as law enforcement officials lack probable cause to obtain a warrant.[14] Can the same be said for Pamela's stored e-mails? It depends.

Because Pamela's e-mails are not retained solely on her hard drive, they are not covered by the Fourth Amendment's protections for personal effects.[15] Instead, statutory provisions typically require law enforcement officials to seek a warrant.[16] According to § 2703 of the Electronic Communications Privacy Act (ECPA), e-mails stored on third-party servers for 180 days or less may not be read by law enforcement officials without a warrant.[17] Because law enforcement

---

server. The convenience of viewing your messages anywhere and nearly unlimited storage spaces makes this option very attractive. Like Pamela, however, users who choose to view and store their emails in this capacity do not enjoy the benefits of Fourth Amendment protections regarding messages they have stored. Instead, the ECPA provides limited protections for these electronic communications. *See* Pegoraro, *supra* note 7; *see*, *e.g.*, Oza, *supra* note 4, at 1053-54.

11 *See* Pegoraro, *supra* note 7.

12 *See id.*

13 U.S. CONST. amend. IV.

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

14 *See id.*; *see, e.g.*, Oza *supra* note 4, at 1044.

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

16 *E.g.*, 18 U.S.C. § 2703(a) (2000).

17 *See id.*

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. *See, e.g.*, Oza *supra* note 4, at 1044.

officials in this example lack probable cause, Pamela's e-mails will remain private for now.[18]

While the e-mails transmitted to Pamela and Kirk's accounts may be identical, after 181 days, law enforcement officials may compel Google to supply the messages delivered to Pamela's account, even if they still lack probable cause to obtain a warrant.[19] Because Kirk's e-mails exist only on his hard drive, they remain protected absent a warrant.[20]

This Comment will demonstrate why the ECPA does not adequately protect privacy interests in electronic content and will suggest that courts should apply Fourth Amendment protections to e-mail content in light of the standards announced in the recent Supreme Court decision, *United States v. Jones*.[21]

Part I of this Comment will briefly examine the background of Fourth Amendment law and Congress's enactment of the ECPA.[22] This Part will also illustrate the deficiencies in the electronic content storage provision of the ECPA.

Part II of this Comment will argue that the deficiencies outlined in Part I may be remedied by an application of Fourth Amendment protections to particular kinds of electronic content and illustrate why e-mail lends itself to property-based protections. Section A will argue that the language in the *Jones* opinion revitalizes the property-based standard to define a Fourth Amendment search. Section B will argue that the answer to ECPA deficiencies is not statutory amendment, but rather an application of the Fourth Amendment standard revitalized in *United States v. Jones*. Finally, Section C will argue that e-mail lends itself to this kind of application because (1) individuals have a right to exclude others from some intangible property spaces, (2) intangible intrusions may be tangible enough to support a trespass to chattels action, and (3) these considerations and reasonable expectations of privacy do not change based on where e-mail is stored.

---

18 *See id.*

19 *E.g.*, Oza, *supra* note 4, at 1045. These kinds of scenarios have raised more than a few eyebrows and have been criticized for drawing arbitrary lines. *See generally id.*

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

21 United States v. Jones, 132 S. Ct. 945 (2012).

22 18 U.S.C. § 2703.

I. THE EVOLUTION OF FOURTH AMENDMENT INTERPRETATION AND THE NEED FOR THE ECPA

This Part will briefly examine the background of Fourth Amendment law and the enactment of the ECPA. Section A will trace the evolution of Fourth Amendment protections from a property-based standard of protection to an expectations-based doctrine. Section B will explore Congress's response to this evolution with its enactment of the ECPA and illustrate the deficiencies in the electronic content storage provision.

Technical changes regarding widely used services, such as e-mail, have forced the Supreme Court to examine two enduring societal clashes; the first being a "desire for privacy" and the practical necessity in participating in wireless communications, and the second regarding the balance between government's "law enforcement needs and people's privacy."[23] Traditionally, the Fourth Amendment has stood as the ultimate measure of this balance, guaranteeing "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[24] From its drafting, the original function and intention of the Fourth Amendment has been to "prohibit government intrusion upon the privacy and property rights of the people."[25]

A purely textual reading of the Fourth Amendment limits its protections to persons, houses, papers and effects, while prohibiting unreasonable searches and seizures.[26] Generally, this means that searches and seizures must be supported by probable cause.[27] Specifically, courts find probable cause to "[search] exists where the facts and circumstances within [the officers'] knowledge and of which they [have] reasonably trustworthy information [are] sufficient in themselves to warrant a man of reasonable caution in the belief that [evidence subject to seizure will be found in the place to be searched]."[28]

---

[23] *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R4521, *UNITED STATES V. JONES*: GPS MONITORING, PROPERTY, AND PRIVACY 1 (2012) [hereinafter THOMPSON II, *GPS Monitoring*].

[24] *See* U.S. CONST. amend. IV; THOMPSON II, *GPS Monitoring*, *supra* note 23, at 1.

[25] *See* THOMPSON II, *GPS Monitoring*, *supra* note 23, at 1.

[26] *See* U.S. CONST. amend IV; JOSHUA DRESSLER & GEORGE C. THOMAS, III, CRIMINAL PROCEDURE: INVESTIGATING CRIME 141 (Thomas Reuters, 4th ed. 2010).

[27] *See* DRESSLER & THOMAS, *supra* note 26, at 141.

[28] *See id.* (citing Brinegar v. United States, 338 U.S. 160 (1949) (alteration in original) (quoting Carroll v. United States, 267 U.S. 132 (1925)).

In these cases, a magistrate will issue a warrant based on probable cause to permit law enforcement officers to lawfully execute a search.[29]

When the Founding Fathers enacted the Fourth Amendment in 1791, they could not have anticipated the scope of technology and resulting communications that would fall outside of the Fourth Amendment's enumerated, protected areas.[30] Even if the Founders desired to prohibit intrusion into these communications, there was simply no way to forecast the invention of the telephone, Internet or e-mail.[31] Intangible modes of communication, which have become part of many daily routines, perhaps as intimately related to our persons as physical letters, do not fit squarely within the objects explicitly enumerated and protected by the Fourth Amendment text.[32] Courts have struggled to deal with intangible property because it does not naturally fall within the scope of original Fourth Amendment protection.[33]

A. *Evolution of Expectations-Based Doctrine: From Common Law Trespass to Reasonable Expectations of Privacy*

Since its enactment in 1791, the Fourth Amendment has evolved from protecting against purely physical trespasses to protecting against violations of an individual's reasonable expectations of privacy.[34] When drafting the language of the Fourth Amendment, the

---

[29] *See id.*

[30] *See* RICHARD M. THOMPSON, CONG. RESEARCH SERV., R42109, GOVERNMENTAL TRACKING OF CELL PHONES AND VEHICLES: THE CONFLUENCE OF PRIVACY, TECHNOLOGY, AND LAW 1 (2011) [hereinafter THOMPSON, *Governmental Tracking*].

[31] *See id.* at 1.

[32] *See id.*; U.S. CONST. amend. IV.

[33] *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (involving e-mail content); eBay, Inc. v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000) (involving robot crawlers mining data on websites); Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003) (involving spam e-mails sent to company e-mail addresses); Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (involving conversion of an internet domain name).

[34] *Compare* Entick v. Carrington, 95 Eng. Rep. 807 (C.P. 1765) *with* Katz v. United States, 389 U.S. 347 (1967).

> For at least the past fifty years, this provision has been subject to more litigation than any other in the Bill of Rights. This may come as no surprise, considering the Fourth Amendment protects, as Justice Brandeis put it, "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." THOMPSON, *Governmental Tracking*, *supra* note 30, at 2 & n.8 (Brandeis J., dissenting) (citing Olmstead v. United States, 277 U.S. 438, 478 (1928)).

Founders intended to guard against general warrants.[35] That is, they despised the practice of government officials invading the home, person and personal effects with broad discretionary powers to search and seize whatever they happened to find.[36] They sought to protect the sanctity of the home, person, and personal effects against unreasonable search and seizures.[37] But as technologies have changed, courts have struggled to square intangible areas and non-physical means of invading spaces with society's reasonable expectations of privacy.[38] The following cases illustrate the evolution of the Fourth Amendment interpretation in the face of these changes.

The law of trespass has traditionally protected privacy by providing tort remedies and criminal penalties for "unauthorized entry" onto another's land.[39] Like other areas of American common law, property law was based on concepts from English common law.[40] *Entick v. Carrington,* "a case considered by many as an ancestor of the Fourth Amendment,"[41] prohibited government officials with a general warrant from searching Entick's home and papers to prove acts of sedition.[42] In this 1765 case, Lord Camden declared that government officials lacked authority to access personal property without permission.[43] The English common law theory of exclusion, which focused

---

35 *See Entick*, 95 Eng. Rep. 807 (C.P. 1765).

36 *See id.*

37 *See id.* at 817 (explaining the significance of property rights in search and seizure analysis: "[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave").

38 *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (involving e-mail content); eBay, Inc. v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000) (involving robot crawlers mining data on websites); Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003) (involving spam e-mails sent to company e-mail addresses); Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (involving conversion of an internet domain name).

39 J. LEE & BARRY LINDAHAL, 4 MODERN TORT LAW: LIABILITY AND LITIGATION § 38:16 (2d ed. 2012). For an annotation collecting and summarizing cases that have been determined under state law and the applicability of common-law actions for trespass to electronic communications, see Marjorie A. Shields, *Applicability of Common—Law Trespass Actions to Electronic Communications*, 107 A.L.R.5th 549 (2003); *see also* RAYMOND S. R. KU & JACQUELINE D. LIPTON, CYBERSPACE LAW 708-09 (Aspen Publishers, 3d ed. 2010) (considering whether common law trespass principles can be applied to information in cyberspace).

40 *See, e.g.*, Entick v. Carrington, 95 Eng. Rep. 807, 817 (C.P. 1765).

41 THOMPSON II, *GPS Monitoring, supra* note 23, at 4.

42 *Id.*; *Entick*, 95 Eng. Rep. at 817-18 (holding that "there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have").

43 *Entick*, 95 Eng. Rep. at 817; THOMPSON II, *GPS Monitoring, supra* note 23, at 4.

largely on the mode of contemplated intrusions, provided the Framers a background for the Fourth Amendment.[44]

A "property-centric approach" was the predominant theory on Fourth Amendment trespass well into early 20th century.[45] In *Olmstead v. United States*, the Supreme Court upheld the validity of warrantless "electronic eavesdropping."[46] In *Olmstead*, law enforcement officials wished to intercept private telephone conversations.[47] To intercept these conversations, they installed wiretaps on wires coming from the house.[48] The Court held that an "actual physical invasion" of the individual's home was needed to constitute a search.[49] In holding that a physical invasion was needed for a Fourth Amendment violation, the Court could find nothing of precedential value that did not rest on trespass to one's property, or "curtilage," or seizure of one's "papers" or "tangible material affects."[50] Since the officers installed the wiretap without trespassing onto Olmstead's property, the Court held this was not an "actual physical invasion" and therefore Olmstead's Fourth Amendment rights had not been violated.[51]

---

44 THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4 ("Under this common law trespass approach, the key inquiry is not necessarily the content of the information obtained by the police, but rather their method of retrieving it.").

45 *Id.*

46 Olmstead v. United States, 277 U.S. 438, 466-67 (1928); *see also* THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4 ("In upholding . . . electronic eavesdropping, the Court ruled that the Fourth Amendment applied only when there was . . . an 'actual physical invasion' of the individual's home.").

47 *Olmstead*, 277 U.S. at 456. The petitioners in this case were convicted of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting and importing liquor. Much of the information that led to the discovery of the conspiracy was obtained by intercepting messages, over the course of many months, on the conspirators' telephones. *Id.* at 456-57.

48 *Id.* at 457-58 ("Small wires were inserted along the ordinary telephone wires from the residences . . . . [T]he insertions were made without trespass upon any property of the defendants."); *see also* THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4 (discussing Olmstead's application of the "property-centric" Fourth Amendment approach).

49 *Olmstead*, 277 U.S. at 466.

50 *Id.*

> Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure. We think, therefore, that the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment.

51 *Id.*

Nearly forty years after *Olmstead*, the Supreme Court noted that the "property-centric approach" had lost credit with the court.[52] In *Warden v. Hayden,* the Court held that "[t]he premise that property interests control the right of the Government to search and seize had been discredited."[53] In fact, some searches and seizures were deemed unreasonable within the language of the Fourth Amendment "even though the Government assert[ed] a superior property interest at common law."[54] As such, the Court recognized that the "principal object" of the Fourth Amendment was no longer "fictional and procedural barriers rested on property concepts."[55] Instead, the Court suggested that privacy should be the focal point of the constitutional inquiry,[56] leading the way for the Court's decision in *Katz v. Untied States*.

In 1967, the Court announced in *Katz* that the "Fourth Amendment protects people, not places."[57] This case involved electronic surveillance of a conversation in a public telephone booth.[58] Although the agents did not physically seize Katz's property, for the recording device was placed on the outside of the telephone booth, the Court held that this surveillance was impermissible.[59] Instead of resorting to a trespassory analysis of the Fourth Amendment, the Court employed a privacy-based analysis, the concurrence announcing that Katz's

---

[52] Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited."); THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4.

[53] *Warden, Maryland Penitentiary*, 387 U.S. at 304; *see also* THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4 (noting that the Court in *Warden, Maryland Penitentiary* suggested that the property-based approach had been "discredited over the years, and that privacy should be the focus of the inquiry under the Fourth Amendment").

[54] *Warden, Maryland Penitentiary*, 387 U.S. at 304.

[55] *Id.*

[56] *Id.*

[57] Katz v. United States, 389 U.S. 347, 351 (1967).

> [T]his effort to decide whether or not a given 'area,' viewed in the abstract, wis 'constitutionally protected' deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. (internal citations omitted).

[58] *Id.* at 348 (This case considered telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth where petitioner placed his calls.).

[59] *Id.* at 353 (holding that the fact that the electronic device employed to achieve that end [intercepting the conversation inside the telephone booth] "did not happen to penetrate the wall of the booth can have no constitutional significance").

"reasonable expectation of privacy" in his conversation in the telephone booth had been violated.[60] Justice Harlan, concurring, suggested a two-prong privacy analysis: (1) Did the individual have an actual (subjective) expectation of privacy? and (2) Was the individual's subjective expectation of privacy objectively reasonable?[61] The *Katz* opinion marked the beginning of the movement away from a property-centered approach for Fourth Amendment search analysis to a reasonableness standard based in expectations of privacy.[62]

B. *Congress Responds to* Katz*: Enacting the ECPA*

Responding to the *Katz* decision, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[63] Title III, "prohibits the unauthorized use of surveillance techniques . . . by public and private actors, but permits law enforcement to use such techniques in controlled and well-defined circumstances."[64] Eighteen years later, Congress enacted the Electronic Communications Privacy Act (ECPA),[65] to provide guidance for law enforcement action and extend protections to subscribers of emerging wireless communications and Internet technologies.[66]

---

[60] *Id.* at 353 (holding that the "Government . . . violated the privacy upon which he [petitioner] justifiably relied"); *id.* at 360-61 (Harlan, J., concurring).

[61] *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

[62] Katz v. United States, 389 U.S. 347, 353 (1976) ("We conclude that the underpinnings of Olmstead and Goldman have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."); *see also* THOMPSON II, *GPS Monitoring*, *supra* note 23, at 4 (discussing the shift from the property-centered approach to the reasonableness standard).

[63] *See* THOMPSON, *Governmental Tracking*, *supra* note 30, at 4 (explaining that Title III is the "core of the federal domestic surveillance law" and covers techniques like bugging and wiretapping); Omnibus Crime Control and Safe Streets Act of 1968, PUB. L. No. 90-351, 82 Stat. 197 (1968).

[64] THOMPSON, *Governmental Tracking*, *supra* note 30, at 4; Omnibus Crime Control and Safe Streets Act of 1968, PUB. L. No. 90-351, 82 Stat. 197 (1968) 82 Stat. 197, §2511.

[65] Electronic Communications Privacy Act of 1986, PUB. L. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2511 (2008)).

[66] *Id.*; S. REP. 99-541, at 1 (1986) ("The Electronic Communications Privacy Act amends title III of the Omnibus Crime Control and Safe Streets Act of 1968 . . . to protect against the unauthorized interception of electronic communications . . . [and] to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

The ECPA has three main parts: (1) the Wiretap Act, (2) the Stored Communications Act, and (3) the Pen Register Act.[67] Under the Stored Communications Act, officers were now required to obtain warrants before intercepting wireless and data communications in transit and in temporary storage.[68] However, in drafting the ECPA, Congress faced difficulties in categorizing e-mails stored with a service provider and deciding how these files should be treated.[69] The Department of Justice took the position that e-mail stored with a service provider was akin to "cold storage" or "abandoned property," if stored long enough.[70] Although this conclusion is not at all intuitive today, storage in 1986 was both limited and expensive.[71] And as a result, servers routinely deleted old e-mails every one to three months.[72] Assuming that those wishing to retain e-mail messages would download the content onto their hard-drive or create a hard copy, Congress decided that e-mail would no longer be protected by the warrant standard after 180 days.[73] Instead, e-mail content older than 180 days would be available to law enforcement agents with a subpoena without judicial approval.[74]

---

67 The Wiretap Act is codified as 18 U.S.C. §§ 2510-2520. The Stored Communications Act is codified as 18 U.S.C. §§ 2701-2712. The Pen Register Act is codified as 18 U.S.C. §§ 3121-3127. The Wiretap Act and the Pen Register Act are not relevant to this discussion and therefore this Comment will only explore the provisions of the Stored Communications Act.

68 18 U.S.C. § 2703 (2000).

69 *Security & Surveillance*: *A Brief History of Surveillance Law*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 21, 2012, 7:00 PM), http://www.cdt.org/issue/wiretap-ecpa (noting that the ECPA "gave email moving over the network essentially the same protection as a phone call or postal letter").

70 *Id.*; *see* U.S. DEP'T OF JUSTICE CRIMINAL DIVISION, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002), available at http://cyber.law.harvard.edu/practicallawyering/Week9DOJECPAExcerpt.pdf.

71 *Security & Surveillance*, *supra* note 69.

72 *Id.*

73 *Id.*; *see also Electronic Communications Privacy Act: Hearing on H.R. 3378 Before Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 475 at 24 (1986) (likening e-mail it to temporary storage boxes for mail and illustrating that drafters of the ECPA did not picture a time when Internet capabilities would allow users to store data permanently on third-party servers).

74 *Security & Surveillance*, *supra* note 69; *see* Robert S. Steere, *Keeping "Private E-mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 255 (1998) (discussing that, unlike warrants supported by probable cause, "an administrative subpoena requires no factual basis and a court order requires a mere offering of 'specific and articulable' facts . . . .").

Nearly twenty-seven years have elapsed since Congress enacted the ECPA.[75] Unsurprisingly, modes of communication have continued to develop and outgrow the "band aid" of protections Congress statutorily provided.[76] One of the most dramatic developments that the ECPA is ill-suited to deal with is the movement of storage to network servers.[77] As Internet access has become "nearly ubiquitous" and the costs of storage have "radically lowered," there has been a considerable trend among individuals to save e-mails to network servers.[78] With the practically unlimited storage space available to users, these e-mails are often read by their intended recipients and stored "indefinitely."[79] In fact, many web-based network servers encourage subscribers not to delete their e-mail messages by advertising nearly unlimited storage space.[80]

Despite the commonplace use of e-mail, the vast majority of e-mail subscribers remain wholly ignorant to the fact that the method in which they read and store their e-mails significantly impacts their privacy rights regarding that content.[81] While having an e-mail address is just as common as having a physical address for much of the U.S. population, not many individuals pay attention to the technical differ-

---

75 The ECPA was enacted in 1986. Electronic Communications Privacy Act of 1986, PUB. L. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 2511 (2008)).

76 *See Security & Surveillance, supra* note 69.

77 *Id.*

78 *Id.*

79 *Id.*

80 Servers like Gmail encourage subscribers to save large amounts of e-mail messages on their server by boasting unlimited free space. *See* Posting of Rob Siemborski to OFFICIAL GMAIL BLOG (Oct. 20, 2012, 6:30 PM), http://gmailblog.blogspot.com/2007/10/more-gmail-storage-coming-for-all.html (stating "[i]n April 2005, we started increasing Gmail storage as part of our "Infinity+1" storage plan. At that time, we realized we'd never reach infinity, but we promised to keep giving Gmail users more space as we were able. That said, a few of you are using Gmail so much that you're running out of space, so to make good on our promise, today we're announcing we are speeding up our counter and giving out more free storage.").

81 Pegoraro, *supra* note 7. The method of delivery can determine how and where e-mails are stored, which directly impacts privacy protections. *See, e.g.*, *Security & Surveillance, supra* note 69.

> [M]ost people now store their emails indefinitely and they store them not on their hard drives but in the cloud, on the servers of their email providers. And people store not only email in the cloud, but also their calendars, their photos, draft documents and a wealth of other sensitive, private data. Any of this data stored on your laptop is fully protected by the Constitution, requiring a warrant for the government to seize it. And as you access the data in real-time over the Internet, your communications are fully protected by ECPA (and also by the Constitution). Yet the same data, sitting in your private, password protected account with a service provider, is available to the government without a warrant under ECPA.

ences between these types of e-mail delivery and storage services.[82] Although the individuals in the above hypothetical registered with the same e-mail provider and read their messages using the same Microsoft program, the difference between POP3 and IMAP delivery choices has lead to a significant difference in the privacy protections of their messages.[83] As previously noted, because Kirk's e-mails are saved and stored solely on his computer's hard drive, he enjoys full Fourth Amendment protection.[84] Pamela, on the other hand, stores her messages on Google's third-party server in addition to her local copy, and must rely on the limited protections provided by applicable provisions of the ECPA regarding the copy on the third-party server.[85]

Title 18 U.S.C. § 2703 lays out "when and how the government may compel a provider of electronic communication service to disclose the contents of an electronic communication, that is in electronic storage."[86] Thus, this section dictates how and when the government may order third party servers to hand over e-mails based on how long the e-mails have remained in storage.[87] What is problematic is that the ECPA protection turns on a distinction between e-mail that has been stored for 180 days or less, and e-mail that has been stored 181 days or more.[88] Subsection (a) of § 2703 states that communications that have been in electronic storage of an electronic communication service for 180 days or less may only be compelled with a warrant requiring probable cause.[89] Subsection (b) deals with communications

---

82 *See* Russell Holly, *Geek 101: Beginners guide to IMAP v.s. PoP*, GEEK (Jan. 20, 2013, 7:20 PM), http://www.geek.com/mobile/geek-101-pop-vs-imap-1536343. According to one study, only 15% of American adult's don't use Internet or e-mail. Kathryn Zickhur, *Who's Not Online and Why*, PEW RESEARCH INTERNET PROJECT (Oct. 13, 2013, 5:30PM), http://www.pewinternet.org/2013/09/25/whos-not-online-and-why/. And, 92% of American Internet users also use e-mail. Kristen Purcell, *Search and email still top the list of most popular online activities*, PEW RESEARCH INTERNET PROJECT (Dec. 10, 2012, 10:45 PM), http://www.pewinternet.org/2011/08/09/search-and-email-still-top-the-list-of-most-popular-online-activities/; *see also* The Radicati Team, *Email Statistics Report, 2011-2015: Executive Summary*, THE RADICATI GROUP, INC. (May 18, 2011), available at http://www.radicati.com/?p=7261 (including global statistics).

83 *See* Pegoraro, *supra* note 7; *see also* Oza, *supra* note 4 at 1052-53 (explaining the delivery and storage differences between IMAP and POP in the presented hypothetical).

84 *See* discussion *supra* Introduction p. 3.

85 *See* discussion *supra* Introduction p. 3.

86 Oza, *supra* note 4, at 1056 (internal quotations omitted); 18 U.S.C. § 2703(a) (2000).

87 Oza, *supra* note 4, at 1056 (internal quotations omitted); 18 U.S.C. § 2703(a) (2000).

88 Oza, *supra* note 4, at 1068-69 (proposing that the best way to protect electronic communications is to erase this distinction); 18 U.S.C. § 2703(a) (2000).

89 18 U.S.C. § 2703(a) (2000).

that are in storage for longer than 180 days.[90] This section states that providers may be compelled to disclose these communications "without required notice to the subscriber . . . if the governmental entity obtains a warrant . . . ."[91] Additionally, providers may still be compelled to disclose in the absence of a warrant if the government gives the subscriber "prior notice" and obtains either an "administrative subpoena . . . or a court order . . . ."[92] Therefore, the standard for a court order is lower than probable cause.[93] To make things worse, the government may also delay notice to the subscriber for up to ninety days if they believe that notification of the court order may have an "adverse result."[94]

Since the trend in communications has shifted to free, web-based email providers that boast nearly unlimited storage capacities, the inapplicability of full Fourth Amendment protections to this data becomes a major issue.[95] In fact, one federal appellate court has held that some provisions of the ECPA are unconstitutional because the provisions allow the government to read a person's e-mail without a warrant.[96]

In *United States v. Warshak*, the United States Court of Appeals for the Sixth Circuit held that the government had violated the defendant's Fourth Amendment rights by compelling his Internet Service Provider to surrender e-mails without providing a warrant.[97] The

---

90 18 U.S.C. § 2703(b) (2000).

91 18 U.S.C. § 2703(b)(1)(A) (2000) (stating that "[a] governmental entity may require a provider . . . to disclose the contents of any wire or electronic communication . . . without required notice to the subscriber . . . if the governmental entity obtains a warrant . . .").

92 18 USC § 2703(b)(1)(B) (2000) (stating that "[a] governmental entity may require a provider . . . to disclose the contents of any electronic communication . . . with prior notice from the governmental entity to the subscriber or customer if the governmental entity . . . uses an administrative subpoena . . . or obtains a court order . . .").

93 18 U.S.C. § 2703(d) (2000) (stating that the standard is merely "specific and articulable facts showing that there are reasonable grounds to believe . . .").

94 18 U.S.C. § 2705(a)(1)(B) (2000); Oza, *supra* note 4, at 1057 (explaining that "[d]elayed notice is an option where notification of the court order may . . . endan[ger] the life or physical safety of an individual, [result] in flight from prosecution, destruction of or tampering with evidence, intimidation of a potential witness, or otherwise seriously jeopardiz[e] an investigation or unduly del[ay] a trial") (internal quotation marks and citations omitted)).

95 Servers like Gmail encourage subscribers to save large amounts of e-mail messages on their server by boasting unlimited, free space. *See* Siemborski, *supra* note 80.

96 United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (declaring that "to the extent that the SCA [Stored Communications Act] purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional").

97 *Id.*

Court explicitly stated that e-mail users maintain "a reasonable expectation of privacy in the content of e-mails" and that the content of these e-mails should be subject to Fourth Amendment protection.[98] To the disappointment of those advocating for e-mail privacy rights, the Court would not apply the exclusionary rule in this case because agents had relied in good faith on provisions of the Stored Communications Act.[99] The *Warshak* holding is still important, however, because of the Court's willingness to hold that violations of users' expectations of privacy in e-mail communications as violations of Fourth Amendment rights.[100]

Even before the *Warshak* decision, the deficiencies in ECPA protections had not gone unnoticed. For years, civil liberties groups and private companies recognized the deficiencies in ECPA protections and began calling on Congress to amend outdated portions.[101] For example, the Digital Due Process Coalition (DDPC), a diverse coalition of privacy advocates, major companies, and think tanks have lobbied Congress to amend outdated portions of the ECPA for years.[102] The DDPC is particularly concerned with those sections relating to e-mail storage.[103] The DDPC points out that many individuals have "years worth of stored email[s]" on the computers of service providers, and that the ECPA sets out inconsistent rules for governmental access to this storage.[104] For example, "a document stored on a desktop computer is protected by the warrant requirement of the Fourth Amendment, but the ECPA says that the same document stored with a service provider may not be subject to the warrant

---

98 *Id.*

99 *Id.* at 292.

100 *Id.* at 288.

101 *See* Rebecca Jeschke, *ECPA Anniversary Brings Calls for Change*, ELECTRONIC FRONTIER FOUNDATION: DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD (Oct. 21, 2012, 5:30 PM), http://www.eff.org/deeplinks/2011/10/ecpa-anniversary-week-brings-calls-change; *see also About the Issue*, DIGITAL DUE PROCESS: MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE (Oct. 21, 2012, 6:28 PM), http://www.digitalddueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163.

102 DIGITAL DUE PROCESS: MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE, *supra* note 101.

103 *Id*. (stating that one of its reform principles is that "[t]he government should obtain a search warrant based on probable cause before it can compel a service provider to disclose a user's private communications or documents stored online.").

104 *Id*. (noting that the "EPCA sets rules for governmental access to email and stored documents that are not consistent. A single email is subject to multiple different legal standards in its lifecycle . . . .").

requirement."[105] This is precisely the distinction between Kirk and Pamela's e-mails in our hypothetical.[106] The DDPC claims that a careful re-write of the problematic areas of the ECPA is needed to provide a clear set of rules for law enforcement access that rids the statute of arbitrary and confusing distinctions, such as the 180 day rule.[107] The bottom line is that this statute is needed to provide a warrant requirement only because intangible data of this sort does not automatically fall within the scope of the enumerated, protected categories of the Fourth Amendment.[108]

When the Supreme Court granted certiorari to hear *United States v. Jones*, many anticipated that the Court would cast light on the status of non-physical intrusions of intangible data.[109] That is, there was hope that the *Jones* opinion would set guidance on the limitations of Fourth Amendment protections as extended to electronic content. As this Comment advocates, if the Court would agree that the Fourth Amendment fully covered this content, there would be no need for additional statutory provisions.

II. ECPA DEFICIENCIES FOR E-MAIL MAY BE REMEDIED BY APPLYING THE FOURTH AMENDMENT INTERPRETATION REVITALIZED IN *JONES*

Part II will argue that the deficiencies outlined in Part I may be remedied by an application of Fourth Amendment protection to particular kinds of electronic content. This Part will also illustrate why e-mail lends itself to traditional, property-based protections. Section A

---

105 *Id*.

106 *See supra* pp. 1-4.

107 DIGITAL DUE PROCESS: MODERNIZING SURVEILLANCE LAWS FOR THE INTERNET AGE, *supra* note 101 (suggesting that instead of attempting "a full rewrite of [the] EPCA, which may have unintended consequences . . . [they are] focus[ed] on just a handful of the most important issues . . .").

108 *See* U.S. CONST. amend. IV (only securing rights in "persons, houses, papers, and effects").

109 *See Supreme Court to Decide Whether GPS Tracking Requires Warrant*, CENTER FOR DEMOCRACY & TECHNOLOGY (Oct. 20, 2012, 9:46 PM), http://www.cdt.org/policy/supreme-court-decide-whther-gps-tracking-receives-warrant (anticipating that the *Jones* decision could impact cell phone tracking); *Supreme Court Agrees to Hear Key Warrantless GPS Tracking Case,* ELECTRONIC FRONTIER FOUNDATION: DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD (Oct. 20, 2012, 10:30 PM), http://www.eff.org/deeplinks/2011/06/supreme-court-agrees-hear-key-warrantless-gps; *see also* Adam Liptak, *Court Case Asks if 'Big Brother' is Spelled GPS*, N.Y. TIMES, Sept. 10, 2011, http://www.nytimes.com/2011/09/11/us/11gps.html.

will begin by arguing that the language in the *Jones* opinion revitalizes the property-based standard to define a Fourth Amendment search. Section B will argue that the answer to ECPA deficiencies is not statutory amendment, but an application of the Fourth Amendment standard revitalized in *Jones*. Finally, Section C will argue that e-mail lends itself to this kind of application because (1) individuals have a right to exclude others from some intangible property spaces, (2) intangible intrusions may be tangible enough to support a trespass to chattels action and (3) these considerations and reasonable expectations of privacy do not change based on where e-mail is stored.

A. Jones *Revitalizes the Property-Based Standard to Define a Fourth Amendment Search*

As previously explained, developments in modes of communication, such as web-based e-mail providers, have complicated traditional Fourth Amendment protections as they do not fit squarely within the enumerated items that demand protection and are not covered by statutory provisions, such as the ECPA.[110] The recent Supreme Court case, *United States v. Jones*, was anticipated to provide some guidance.[111] In January of 2013, the Court announced a holding based on a physical intrusion approach rooted in traditional property law trespass doctrine.[112] While many have speculated on how this decision applies to intangible data and privacy expectations,[113] *Jones* itself does not explicitly address instances where the government engages in behavior that does not involve physical intrusion onto intangible property.[114] Thus, a re-conceptualization of electronic content and electronic spaces will be key to making this holding applicable to spaces like e-mail.

Before *Jones*, the Supreme Court cultivated a Fourth Amendment analysis that moved away from a property-centered approach, to a test that relied on an individual's reasonable expectations of pri-

---

110 *See* discussion *supra* Part I.B., pp. 11-14.

111 *See* sources cited *supra* note 109.

112 United States v. Jones, 132 S. Ct. 945, 953-54 (2012) (holding that the warrantless attachment of a GPS device to a vehicle constituted a search and classic Fourth Amendment violation).

113 *See, e.g.*, CENTER FOR DEMOCRACY & TECHNOLOGY; *Supreme Court to Decide Whether GPS Tracking Requires Warrant*, *supra* note 109.

114 *See Jones*, 132 S. Ct. at 953-54 (holding instead that the physical attachment of the GPS device constituted the warrantless search).

vacy.[115] The Court advanced the reasonableness test in the seminal *Katz* case, announcing that "the Fourth Amendment protects people, not places."[116] However, the *Jones* opinion arguably created the logical foundation for the revitalization of a property-focused analysis.[117] *Jones* did not squarely address Fourth Amendment protections for intangible data. Even so, if the Court is willing to recognize true property rights in particular forms of electronic communication and Internet spaces, the property-centered approach relied on in *Jones* will afford bright-line protections for these intangible interests, regardless of the mode of interception used.

Concededly, and to the disappointment of many privacy rights advocates, the Supreme Court did not squarely address the issue of Fourth Amendment protections against non-physical intrusion on intangible data.[118] *Jones* concerned prolonged Global Positioning System (GPS) tracking of a criminal suspect's vehicle.[119] The highly anticipated decision left many critics complaining that the Court strategically sidestepped these technological issues.[120] Far from handing down guarantees of protection for digital data and prohibiting modes of non-physical government intrusion, the Court focused on the actual physical intrusion of the tracking device at issue in this case, drawing on pre-*Katz* considerations of physical trespass grounded in property law.[121]

---

115 *See* discussion *supra* Part I.A., pp. 7-10.

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

117 *See Jones*, 132 S. Ct. at 953 ("What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted."); *see also* Erica Goldberg, *How* United States v. Jones *Can Restore our Faith in the Fourth Amendment*, 110 MICH. L. REV. 62, 62 (2011) (arguing generally that a property-rooted Fourth Amendment analysis will provide stability for this area of law and that Jones provides the basis to restore this pre-1967 framework).

118 *Jones*, 132 S. Ct. at 954 ("We may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here."); *see, e.g.*, Jim Patterson, *High Court's GPS Decision Sidesteps Larger Privacy Question: Vanderbilt Expert*, VANDERBILT NEWS (Oct. 15, 2012, 8:30 PM), http://news.vanderbilt.edu/2012/01/slobogin-gps-scotus/ (pointing out that "much government tracking does not involve the use of a device planted on a car"); Daniel J. Solove, United States v. Jones *and the Future of Privacy Law: The Potential Far-reaching Implications of the GPS Surveillance Case*, PRIVACY & SECURITY LAW REPORT (BNA 2012) (claiming that the majority "did not analyze whether there was a reasonable expectation of privacy in this case") [hereinafter Solove, *United States v. Jones*].

119 *Jones,* 132 S. Ct. at 948 (involving monitoring of suspect's car for twenty-eight days).

120 *See* sources cited *supra* note 118.

121 *Jones*, 132 S. Ct. at 949 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have

The Court agreed that a search occurred when law enforcement officers attached a GPS tracking device to the undercarriage of Jones's Jeep and tracked his movements for four weeks.[122] Although the officers had obtained a search warrant, they attached the device outside of the jurisdiction where the warrant was issued and executed the warrant after its prescribed time frame expired.[123] While unanimous in outcome, the Court could not agree on what conduct actually constituted the search.[124] Using the *Katz* analysis, Justice Alito, concurring with the majority, argued that the length of the monitoring exceeded Jones's reasonable expectations of privacy.[125] In a somewhat surprising contrast, Justice Scalia, writing for the majority, held that the physical attachment of the GPS device and the subsequent attempt to obtain information constituted the violation.[126]

The Court did not focus on Jones's reasonable expectation of privacy in his movements; rather, the Justices emphasized the physical intrusion occasioned by the actual attachment of a GPS monitoring device to the vehicle.[127] Since Jones's car was an "effect," the attachment constituted a physical intrusion into a constitutionally protected area.[128] This physical intrusion, coupled with the attempt to gain

---

been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."); *see id.* at 957-58 (Alito, J., concurring) ("By attaching a small GPS device to the underside of the vehicle . . . the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels . . . [a]nd for this reason . . . the installation and use of the GPS device constituted a search.").

122 *Id.* at 949.

123 *Id.* at 948 (noting that the warrant authorized the installation of the device in the District of Columbia within ten days, but the actual installation occurred on the eleventh day in Maryland).

124 *Infra* notes 125, 126 and accompanying text.

125 *Jones*, 132 S. Ct. at 957-58 (Alito, J., concurring) (finding that the majority's holding unwisely strains the language of the Fourth Amendment and arguing that the Court should analyze the question presented by asking whether or not the suspect's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove").

126 *Id.* at 949 (emphasizing that "[t]he Government physically occupied private property for the purpose of obtaining information.").

127 *Id.* ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"); *see also id.* at 954 (Sotomayor, J., concurring) ("I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, where as here, the Government obtains information by physically intruding on a constitutionally protected area.") (internal quotations omitted).

128 *Id*. at 949 (emphasizing "a vehicle is an 'effect' as that term is used in the Amendment").

information, amounted to a search.[129] Without a valid warrant, this search was unconstitutional under the Fourth Amendment.[130]

As Justice Alito noted in his concurrence, and as this Comment advocates, this theory hinges on common law trespass, as it existed when the Fourth Amendment was adopted.[131] The outcome in *Jones* does not follow the recent post-*Katz* case law that relies on a subjective conception of privacy.[132] Instead, Jones's property rights in his car defined his right to be free from government intrusion.[133] In other words, Jones had the right to exclude the officers from trespassing on his property.

It is important to note that Justice Scalia claims the majority opinion in *Jones* does not reflect an overruling of *Katz*. In fact, he suggests that physical trespass and reasonableness analyses run in tandem.[134] Where physical trespass is not involved, the Court will look to an individual's reasonable expectations of privacy to decide whether a search has been conducted.[135] Thus, Jones was not "searched" because he had a reasonable expectation of privacy in a constitutionally protected area, but rather because warrantless, physical trespass onto private property is the quintessential mark of a Fourth Amendment violation.[136]

Despite Scalia's claim that physical trespass has always run in tandem with the reasonableness analysis, this understanding is not echoed in prior cases.[137] The Court's reliance on physical trespass does not appear to follow the precedential trend away from a prop-

---

129 *Id.*

130 U.S. CONST. amend. IV.

131 *Jones,* 132 S. Ct. at 957 (Alito, J., concurring) (stating that "by attaching a small GPS device to the underside of the vehicle . . . law enforcement officers . . . engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels . . . [a]nd for this reason, the Court concludes the installation and use of the GPS constituted a search").

132 *Id.* at 958 (suggesting that the majority's holding is "unwise" because "[i]t strains the language of the Fourth Amendment . . . has little if any support in current Fourth Amendment case law [and is] highly artificial.").

133 *Id*. at 949 (emphasizing "a vehicle is an 'effect' as that term is used in the Amendment").

134 *Id.* at 951-52 (stating that the Court in *Katz* held that "property rights are not the sole measure of Fourth Amendment violations," but did not "snuf[f] out the previously recognized protection for property" . . . for the "*Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test.").

135 *Id.* at 950.

136 United States v. Jones, 132 S. Ct. 945, 949-50 (2012).

137 *See supra* note 131 and accompanying text.

erty-based analysis.[138] For example, in 1967, the Court specifically stated that,

> [t]he premise that property interests control the right of the Government to search and seize has been discredited. Searches and seizures may be 'unreasonable' within the Fourth Amendment even though the Government asserts a superior property interest at common law. We have recognized that the principal object of the Fourth Amendment is the protection of privacy rather than property, and have increasingly discarded fictional and procedural barriers rested on property concepts.[139]

Thus, by reviving a property-based test and specifically relying upon it, the Court indicated its willingness, if not desire, to return to a property rooted Fourth Amendment analysis. At the very least, by focusing on the physical intrusion in this case, the Court created the logical basis for a revitalization of a property-rooted analysis. The Court may become more amenable to a property-rooted analysis of Fourth Amendment protections in the future because the standard may prove to be more reliable in the face of continually changing social perceptions as to what constitutes reasonable expectations of privacy.[140]

As technology continues along its trajectory of rapid growth and change, the Court will see the usefulness in bright line rules, and the *Jones* case will serve as the platform for shifting back to a property based Fourth Amendment approach. Although the property based approach may seem fatal to electronic content that does not fit squarely within the enumerated, protected objects of the Fourth Amendment, as the next section of this comment will suggest, a property based analysis may provide greater protection for electronic content than a reasonable expectations based analysis has in the past. As the following section argues, real property rights, such as the right to exclude others, already exist in particular forms of electronic content,

---

138 *See, e.g.*, Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 304 (1967); Katz v. United States, 389 U.S. 347, 353 (1967).

139 *Warden, Maryland Penitentiary*, 387 U.S. at 304.

140 *Jones*, 132 S. Ct. at 963 (Alito, J., concurring) (noting that "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes" and that the expectation-of-privacy test will suffer from these difficulties); *see also* Goldberg, *supra* note 117 (arguing generally that a property-rooted Fourth Amendment analysis will provide stability for this area of law).

and intangible intrusions into these spaces have been deemed actionable through physical trespass doctrines.[141] Therefore, instead of deciding on a case-by-case basis whether individuals maintain reasonable expectations of privacy in their electronic content in the face of changing societal perceptions surrounding access to and security in their digital information, a property-based Fourth Amendment standard will provide predictable rulings when spaces—where individuals have a right to exclude others—have been intruded upon in ways that are tangible enough to be actionable under real property doctrines, such as trespass to chattels.

B. *The Answer to ECPA Deficiencies is Not Amending the ECPA but Revisiting the Applicability of Fourth Amendment Protections*

Pre-*Jones* scholars have been addressing deficiencies in the ECPA and elsewhere long before the Court announced it would consider *United States v. Jones*.[142] In fact, Congress itself proposed amendments to the ECPA; however none of these amendments were aimed at the electronic storage provision that this Comment addresses.[143] Regardless, when viewing the protective gaps in the ECPA language, the answer was always the same: Congress needs to amend it.[144] Although things like e-mail are not tucked neatly under

---

141 *See, e.g.*, eBay v. Bidder's Edge, 100 F.Supp.2d 1058, 1069-70 (N.D. Cal. 2000) (holding that using automated crawlers, or computer robots, to download information from websites can constitute a trespass to chattels); Kremen v. Cohen Network Solution, Inc., 337 F.3d 1024, 1030 (9th Cir. 2003) (finding that an Internet domain name was a form of intangible property which could serve as the basis for registrant's conversion claim); Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1348-50 (2003) (finding that sending spam e-mails could constitute a trespass to chattels).

142 *See generally* Oza, *supra* note 4, at 1054-56; *see also* Steere, *supra* note 74, at 233 (advocating modifications to the ECPA to provide equal privacy protection to all communication "in order to encourage the growth and use of emerging communication technologies."); Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMMLAW CONSPECTUS 129 (2011) (arguing that Congress should adopt reforms proposed by the Digital Due Process Coalition in order to bring the provisions "into the 21st century"); Orin S. Kerry, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (specifically arguing that Congress should (1) raise the threshold the government must satisfy to compel the contents of certain Internet communications; (2) simplify the statue; (3) repeal 18 U.S.C. § 2701; and (4) restructure the remedies scheme for violations of the statute).

143 *See* H.R. 3156, 110th Cong. § 131 (2007).

144 For a detailed discussion see Oza, *supra* note 4, at 1068-71 (advocating for amendments to the ECPA); *see also, e.g.*, Steere, *supra* note 74, at 274.

the Fourth Amendment umbrella, given a purely textual reading of the amendment, these types of communications have become integral to the common experience of daily living and equally as deserving of privacy protections as those enumerated objects.

Although the view that Congress is best suited to make factual determinations instead of the Court is well-founded,[145] the ECPA, in many respects, has served as a confusing and complicated "band aid" for Fourth Amendment protection gaps regarding communications the Founders did not and could not have foreseen. Arguably, amending the outdated portions of the ECPA would be like replacing a band-aid with a fresh one. This temporary fix would leave courts with a law that would inevitably become outdated and ineffective. Because developments in communications are likely to continue, this new patchwork would become outdated and as equally hard to apply as the original provisions. In contrast, applying Fourth Amendment protections to electronic spaces that meet common sense criteria would result in bright line protections, giving the courts reliable standards and the general public assurances e-mail communications will remain protected in the manner that they would expect privacy in other personal effects. Scalia's application of tandem running approaches in *Jones* indicates that the Court may indeed move in this direction.[146]

---

[145] *See* Oza, *supra* note 4, at 1069 (citing Erin E. Wright, *The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of* Warshak v. United States, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 531, 544 (2008) (explaining that scholars argue that the legislature, not the courts, should determine privacy rights in the face of rapidly changing technology)). *But see id.* at n.191 (citing Erin E. Wright, *The Right to Privacy in Electronic Communications: Current Fourth Amendment and Statutory Protection in the Wake of* Warshak v. United States, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 531, 549 (2008) (stating that "[p]roponents . . . argue that the courts should determine the outer limits of government surveillance")).

[146] United States v. Jones, 132 S. Ct. 945, 951-52 (2012) (stating that the "Katz reasonable-expectation-of privacy test has been *added to,* not *substituted for,* the common-law trespassory test").

C. *E-mail Lends Itself to a Fourth Amendment Application because (1) E-mails are Spaces where Individuals have the Right to Exclude Others (2) Reading E-mails Is Intrusively Tangible to Support a Trespass to Chattels Cause of Action, and (3) Where E-mail is Stored does not change Claim (1) or (2)*

Real property rights, such as the right to exclude others, are already recognized in some forms of intangible data.[147] Historically, courts have recognized these real property rights in domain names.[148] While domain name spaces diverge in obvious ways from parcels of land or objects capable of being touched, courts have recognized that in some cases individuals have analogous rights in these nonphysical spaces.[149] Although these cases involve nonphysical intrusions on intangible property, courts have applied the real property doctrine of trespass to chattels when intrusions have occurred.[150] Trespass to chattels provides a cause of action "where an intentional interference with the possession of personal property has proximately cause[d] injury."[151]

For example, in 2000, eBay successfully used the "trespass to chattels" theory to obtain a preliminary injunction against Bidder's Edge.[152] The defendant in this case used a "crawler" program to compile auction data from eBay's auction website.[153] Without eBay's permission, the program accessed the auction website with a high degree

147 *See, e.g.*, Kremen v. Cohen Network Solution, Inc., 337 F.3d 1024, 1030 (9th Cir. 2003) (finding that an Internet domain name was a form of intangible property which could serve as the basis for registrant's conversion claim); eBay v. Bidder's Edge, 100 F.Supp.2d 1058, 1069-70 (N.D. Cal. 2000) (holding that using automated crawlers, or computer robots, to download information from websites can constitute a trespass to chattels); Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1348-50 (2003) (finding that sending spam e-mails could constitute a trespass to chattels).

148 *See, e.g.*, *Kremen*, 337 F.3d at 1030 (9th Cir. 2003); *eBay*, 100 F.Supp.2d at 1069-70; *Intel Corp.*, 30 Cal. 4th at 1348-50.

149 *See, e.g.*, *Kremen*, 337 F.3d at 1030 (9th Cir. 2003); *eBay*, 100 F.Supp.2d at 1069-70; *Intel Corp.*, 30 Cal. 4th at 1348-50.

150 *See, e.g.*, *Kremen*, 337 F.3d at 1030 (9th Cir. 2003); *eBay*, 100 F.Supp.2d at 1069-70; *Intel Corp.*, 30 Cal. 4th at 1348-50.

151 *See* BLACK'S LAW DICTIONARY 1643 (9th ed. 2009) (defining "trespass to chattels").

152 eBay v. Bidder's Edge, 100 F.Supp.2d 1058, 1073 (N.D. Cal. 2000).

153 *Id.* at 1062 ("BE [Bidder's Edge] wanted to recursively crawl [using software robot programs] the eBay system to compile its own auction database . . . [which would allow] BE to track the auctions generally and automatically update its users when activity occurs in particular auctions . . . or when new items are added.").

of frequency to mine and aggregate data.[154] To obtain a preliminary injunction, eBay had to meet the pre-requisite showing that they possessed a true intangible property interest to exclude others from using the site in undesirable ways.[155] By granting the preliminary injunction, the district court suggested that eBay had a property interest in excluding others from its website much like the interest in prohibiting trespassers to chattels.[156]

That same year, the Ninth Circuit similarly held in *Kremen v. Cohen Network Solutions, Inc.* that the registrant of an Internet domain name had an intangible property right which carried with it real property implications.[157] In this case, Kremen sued for conversion to recover losses related to the erroneous reassignment of the domain name "sex.com" to another registrant.[158] The tort of conversion raises the preliminary question of whether a true property right existed in what plaintiff claims was allegedly converted.[159] The circuit court held that plaintiff's Internet domain name satisfied property right criteria because registrant was (1) capable of exclusive control (2) of a precisely defined interest (3) from which he legitimately had the right to exclude others.[160] Thus, this case marked a legitimate property interest in an intangible good, and the wrongful disposition of that domain name constituted the tort of conversion.[161]

---

154 *Id.* at 1063 (conceding that the crawlers accessed the eBay site approximate 100,000 times a day).

155 *Id.* at 1066-67 (concluding that "under the circumstances present here, BE's ongoing violation of eBay's fundamental property right to exclude others from its computer system potentially causes sufficient irreparable harm to support a preliminary injunction.").

156 *See id.*

157 Kremen v. Cohen Network Solution, Inc., 337 F.3d 1024, 1030 (9th Cir. 2003) (applying a three part test to determine whether property rights exist and determining that domain names satisfy each criterion).

158 *Id.* at 1027-28.

159 *Id.* at 1029.

160 *Id.* at 1030.

> Like a share of corporate stock or a plot of land, a domain name is a well-defined interest. Someone who registers a domain name decides where on the Internet those who invoke that particular name—whether by typing it into their web browsers, by following a hyperlink, or by other means—are sent. Ownership is exclusive in that the registrant alone makes that decision. Moreover, like other forms of property, domain names are valued, [as they are] bought and sold.

161 *Id.* at 1036.

1. E-mails Should be Spaces Where Individuals Have the Right to Exclude Others: Applying the *Kremen* Standard

Not only did the Sixth Circuit Court of Appeals in *United States v. Warshak* explicitly state that users maintain "a reasonable expectation of privacy in the contents of [their] emails," but this expectation of privacy flows from a real property right in this content.[162] This subsection will apply the standard used in *Kremen* to support this claim.[163]

In *Kremen*, the Court held that the plaintiff's Internet domain name satisfied property right criteria because the registrant was (1) capable of exclusive control (2) of a precisely defined interest (3) from which they legitimately had the right to exclude others.[164] Third-party e-mail services, such as Gmail, have the ability to scan, manipulate, or otherwise access a subscribers' messages and mail behavior for the purposes of spam filtering, monetizing via targeting advertisements, or for any number of other actions as allowed by the Terms of Service agreed upon the subscriber when signing up for the service.[165] However, outside of this, e-mail subscribers themselves are capable of maintaining exclusive control over their e-mails. They have the option to download e-mail content from third-party servers via the IMAP or POP3 protocols. While this content remains on third-party servers if the IMAP protocol is chosen, subscribers have the option to password-protect this access point to keep others from viewing or copying the content within.[166] Additionally, e-mails are not broad limitless concepts. They are discrete files, whose boundaries can be precisely defined.[167] The interest in protecting e-mails can also be pre-

---

162 United States v. Warshak, 631 F.3d, 266, 287-88 (6th Cir. 2010).

163 Kremen v. Cohen Network Solution, Inc., 337 F.3d 1024, 1030 (9th Cir. 2003).

164 *Id.*

165 *See, e.g.*, About Google- Policies and Principles, GOOGLE, www.google.com/intl/en/policies/terms/ (follow the "About Google" hyperlink then follow the "Privacy and Terms" hyperlink).

166 *See,* e.g., Gmail Help- Change your Password, GOOGLE, https://support.google.com/mail/answer/6567?hl=en (follow the "Gmail" hyperlink then follow the "Help" hyperlink, then follow the "Change your Google Account Password" hyperlink); Yahoo Help- Change your Password, YAHOO, https://help.yahoo.com/kb/password-sln2035.html (follow the "Help" hyperlink then follow the "My Account" hyperlink and then follow the "Change your Password" hyperlink).

167 E-mail messages are discrete computer files, similar to .mp3 music files or .doc Microsoft Word document files. E-mail messages were originally formatted as plain ASCII text, but various committees and organizations gradually amended this. The current format, estab-

cisely defined in terms of exclusion—the most important stick in the bundle of property interests.[168] Lastly, individuals have a legitimate right to exclude others from private content existing in e-mail correspondence. This notion is not only popularly accepted, but also confirmed in Congress's attempt to protect electronic communications through particular provisions of the ECPA.[169] Therefore, e-mail meets the property criteria set out in *Kremen*, which considered whether a true property right existed in converted e-mails.[170] According to the *Kremen* standard, it seems clear that individuals should be deemed to have a true property right in e-mails and e-mail contents.

2. Reading E-mails Is Intrusively Tangible to Support a Trespass to Chattels Cause of Action

To sustain an action for trespass to chattels, the space must not only be an area where an individual has a true property right and thus has a legitimate right to exclude others, but the intrusion into the space must be tangible enough to support the trespass cause of action.[171]

In the 2003 case of *Intel Corp. v. Hamidi*, the California Supreme Court held that under California law, the tort of trespass to chattels did not encompass an electronic communication that neither damaged the recipients computer system nor impaired its functioning.[172] Hamidi, a former Intel employee repeatedly sent a large number of e-mails to current employees criticizing the company, even after the

---

lished in 2008, is a combination of the formats RFC 5322 and RFC 2045-2049, known collectively as the Multipurpose Internet Mail Extensions, or MIME. Modern email formatting standards such as this allow for additions to the original text-only ASCII e-mail standard, such as rich text formatting, hyperlinking, in-line photos and videos, and various types of multimedia and document attachments. *See* Posting of Ken Simpson to MailChannels, *An update to the email standards*, www.mailchannels.com/blog/2008/10/an-update-to-the-email-standards/ (Nov. 28, 2012, 8:46 PM).

168 *See* BLACK'S LAW DICTIONARY 1335-36 (9th ed. 2009) (defining "property").

169 *See generally* 18 U.S.C. § 2703(a) (2000).

170 *See* Kremen v. Cohen Network Solution, Inc., 337 F.3d 1024, 1030 (9th Cir. 2003) (applying a three part test to determine whether property rights exist).

171 *See* BLACK'S LAW DICTIONARY 1643 (9th ed. 2009) (defining "trespass to chattels").

172 Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1353 (2003).

> [In] applying the tort of trespass to chattels to various types of unwanted electronic contact between computers . . . [we are not persuaded] that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have generally involved some actual or threatened interference with the computers' function.

company requested that Hamidi cease these communications.[173] In response to the messages and alleged workplace disruption, Intel asserted that the communications constituted a trespass to chattels under California law.[174] Absent actual damage and causation, the suit failed in California because the trespass to chattels tort could not be proven without evidence of damage to the plaintiff's property.[175] The Court noted that if the quantity of e-mails escalated to the degree of impairing Intel's computer, a trespass to chattels action suit could prevail.[176] The point here is that nonphysical electronic transmissions, such as e-mail or similar intrusions onto excludable spaces, may be actionable under common law property theories because they are "tangible" enough to constitute an intrusion.[177]

Seven years earlier, the California Court of Appeals for the Fourth District applied the trespass to chattels doctrine to cover the unauthorized use of long-distance telephone lines.[178] In *Thrifty-Tel v. Bezneck*, the Court noted that "the electronic signals generated by the . . . activities [was] sufficiently tangible to support a trespass cause of action."[179] While the *Jones* case turned on the physical attachment of a GPS tracking system to the undercarriage of a car,[180] the idea present in *Thrift-Tel, Inc. v. Bezenek* is the same. Both cases involve instances of unauthorized "tangible" intrusions into spaces where individuals had a legitimate right to exclude others. In *Jones*, Justice Alito recognized that courts have held "the transmission of electrons that occurs when a communication is sent from one computer to another is enough" to constitute trespass to chattels.[181] Logically, if the unauthorized use of a telephone line is sufficiently tangible to sup-

---

173 *Id.* at 1346.

174 *Id.* at 1346-47.

175 *Id.* at 1360.

176 *Id.* at 1348.

177 *See, e.g.*, CompuServe, Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015, 1022 (S.D. Ohio 1997) (approving the use of trespass to chattels as a theory of spammer's liability to ISP's based upon evidence that the vast quantities of mail sent by spammers both overburdened the ISP's own computers and made the entire computer system harder to use for recipients).

178 Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1564-66 (1996) (noting that although trespass to chattel is "seldom employed as a tort theory" in California, it does lie "where an intentional interference with the possession of personal property has proximately caused injury.").

179 *Id.* at 1566 n.6.

180 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Alito, J., concurring).

181 *Id.* at 962.

port a trespass cause of action, the unauthorized viewing and copying of e-mail should also be actionable.

3. A Property-Based Fourth Amendment Standard Should Provide Full Fourth Amendment Protections to E-mail Regardless of Where it is Stored Because Where E-mail is Stored Does not Change Claim (1) or (2)

As Section B demonstrated, e-mail is a space where individuals have the right to exclude others and reading or acquiring copies of these e-mails may be tangible enough to support a trespass to chattels cause of action. This Comment advocates that these factors do not change depending on where the e-mail is stored. That is, these factors are independent of any distinctions between storage on personal computers, as Kirk did in the hypothetical, and storage on third-party servers, as the hypothetical showed Pamela doing. Although a third-party may have physical control of e-mails in the second scenario, Pamela should have the same expectation of privacy in her e-mail as Kirk. She has not availed its content, but only shared particular attributes relating to the message in order for it to be sent to another computer. For purposes of Fourth Amendment search considerations, this information is considered "envelope" information, not content information.[182] The Supreme Court has held that although individuals do not have a reasonable expectation of privacy in "envelope" information, sharing this information with third parties does not extinguish a right to Fourth Amendment protection regarding content information.[183]

In 1976, the United States Supreme Court famously held in *Smith v. Maryland* that installation and use of a pen register by a telephone

---

[182] *See* Oza, *supra* note 4, at 1049-50 (demonstrating that the content/envelope distinction allows courts to recognize "that while a third party may have physical control over an individual's information, such control does not make all expectations of privacy unreasonable."). For an in-depth discussion of content/envelope information and third party doctrine see Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 2 (Spring 2007); *see also* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law* 50 WM & MARY L. REV. 2105 (2009).

[183] Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (stating only that the Fourth Amendment does not prohibit obtaining information revealed to a third party, even if revealed on assumption that the information would be used for a limited purpose).

company did not constitute a "search" within the meaning of the Fourth Amendment.[184] Since the pen register only recorded numbers dialed, which the individual knew to be necessarily exposed to the third party to make the telephone call, the caller did not maintain a reasonable expectation of privacy in this information.[185] The Fourth Amendment protected the conversation, but not the numbers dialed before that conversation occurred.[186] Therefore, the Fourth Amendment protection extended to the content of the communication, not the "envelope."[187] Analogizing these terms to the context of e-mail communication, the message body becomes the content, while the other fields, which help e-mail transfer from one computer to another becomes the envelope information.[188] Thus, when Pamela allows her e-mail to remain on a third-party server she conveys particular pieces of information to that third party.[189] The third party knows the address of the sender, the subject-line text of the e-mail and the size of the message.[190] Without reading the e-mail, the third party does not know its content.

The distinction between content and envelope information was a central issue in *United States v. Forrester*.[191] In *Forrester*, the Ninth Circuit held that the warrantless monitoring of addresses to and from defendant's account did not violate defendant's Fourth Amendment rights.[192] This was "envelope" information. The Court also stated that "the Supreme Court has held that the government cannot engage in warrantless search of the contents of sealed mail, but can observe

184 *Id.* at 745-46 ("We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.' The installation and use of the pen register, consequently, was not a 'search,' and no warrant was required.").

185 *Id.* at 743-46.

186 *Id.* at 742.

187 *See id.*

188 Oza, *supra* note 4, at 1057. ("Examples [of other fields] are the 'to' address, the 'from' address, the sender's and receiver's IP addresses, and the time and date stamp."); *see also* sources cited *supra* note 182.

189 *See generally* Oza, *supra* note 4, at 1057-58; *see also* sources cited *supra* note 182.

190 *See* Oza, *supra* note 4, at 1057.

191 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008); *see* Oza, *supra* note 4, at 1057-58 (discussing the content/envelope distinction at issue with co-defendants e-mail correspondences).

192 *Forrester*, 512 F.3d at 510 (finding that e-mail to/from addresses and IP addresses "constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers," which are not protected by the Fourth Amendment).

whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties."[193]

Although in Pamela's case, she has done more than voluntarily transmit information regarding the sender and size of the e-mail to third parties by storing the messages on a Google server, Google's physical control should not make her expectations of privacy unreasonable. This Comment advocates the position that because Pamela has given the third party access to the envelope information, it does not follow that hidden content information has also been surrendered.[194] Because the subscriber has a true property interest in the contents of the e-mail, where the e-mail is stored should not alter the individual's Fourth Amendment protections.

CONCLUSION

United States v. Jones does not provide clear guidance for Fourth Amendment protections for intangible property interests nor speak to the permissibility of warrantless, non-physical government intrusions into these spaces. However, if the Court is willing to recognize true property rights in particular forms of electronic communication, the property-centered approach relied on in *Jones* will afford bright-line protections for these intangible interests, regardless of the mode of interception used.

---

[193] *Id*. at 511 (noting that "[t]he government's surveillance of e-mail addresses . . . may be technologically sophisticated, but . . . is conceptually indistinguishable from government surveillance of physical mail.").

[194] United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010) (arguing that the constitutional analysis applied both to e-mails stored privately and publicly) (internal citations omitted).

> While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private . . . Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection.