Inefficiency of the U. S. Electronic Communications Privacy Act of 1986 to Protect Citizen's Privacy Rights on Stored Electronic Communications: A Proposal to Modify It.

By: Pablo Gaspar Arosemena G.
Arosemena & Asociados.

I. Introduction.

Our modern society is directly influenced by several technological advances that shape their growth and affect every single aspect of its development. This technology entails the enactment of legal provisions to regulate their application and deal with legal problems that could arise. One type of technology that makes possible this social growth is "cyber communication." It can be transferred through different means such as the Internet. One of the infinite uses of cyberspace is the transmission of electronic mail, or e-mail.[1] This communication mean is covered or described by the same statutory definition that defines "electronic communication."[2] E-mail is essentially the core of on-line activity, because it comprises the most common, basic function that allows individuals to correspond with one another via computers.[3] It is in this electronic environment that the issue of electronic communications privacy arises. Thus, digital technology creates exposure and possible intrusion from individuals or the government to different electronic communications, such as e-mails. The exposure creates a risk of intruders violating a privacy interest or engaging in fraud or manipulation.[4] Citizens consider this privacy interest as a fundamental right, right to

[1] Robert S. Steere, Note, *Keeping "Private E-mail" Private*, 33 VAL. U. L. REV. 231 (1998).
[2] 18 U.S.C. § 2510 (12) defines "electronic communication": any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but does not include – (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.
[3] See supra note 1 for the definition of "electronic mail" or "e-mail."
[4] Raymond T. Nimmer, Information Law, page 8-36 (2001).

maintain confidentiality on their communications, avoiding improper violation of their right protected by U.S. constitutional and statutory provisions such as the Fourth Amendment of the United States Constitution and the Electronic Communications Privacy Act of 1986 ("ECPA"). As stated before, these provisions are necessary to protect citizen's privacy rights from government intrusion, specifically in the electronic communication area, usually related to abuses in the detection and prosecution of criminal activities, as well as from individual intrusion. Despite the foregoing, the ECPA is not currently fulfilling the mission for what it was enacted, full protection of electronic communications, specifically in the area of stored electronic communications. In this sense, concrete legislative measures should be taken to fix this gap, which is affecting one of people's fundamental personal rights.

Regarding the content of this brief paper, I will first state the Background of this main issue, how the U.S. Fourth Amendment and the Electronic Communications Privacy Act of 1986 (specially chapters I and II) constitute the federal constitutional and statutory provisions for the protection of the individual's right to **"be let alone"** and the current restrictions for government intrusion on cyber communications, specifically stored electronic ones.

In the following section I will focus on the specific ECPA Title II provisions that establish restrictions and protections from government intrusion in **"stored" electronic communications**, but at the same time, fail to provide enough privacy protection. I will also examine proposals by which the U.S. Congress could amend ECPA in order to offer stronger protection for privacy interests, in this case, private e-mails.

Finally, I would indicate my conclusion on this issue.

II. Background.

The United States Fourth Amendment and the Electronic Communications Privacy Act of 1996 vs. Government Intrusion Problem.

A. Federal Constitutional Provision: The Fourth Amendment.

The Fourth Amendment of the United States Constitution constitutes the initial legal provision in the never-ending search for protection of privacy interests. It indicates that "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.[5]

This provision also constitutes the legal framework for the enactment of several federal and state laws guided to regulate this important matter, establishing civil and criminal law protections to attempt to establish a security environment. Hence, this federal constitutional law regulates searches and seizures by governmental entities in areas within an individual holds a reasonable expectation of privacy.[6] According to professor Nimmer, the communications environment contains a reasoned and reasonable expectation of privacy[7], derived from the fact that a computer (communication environment) is not an open forum or unit unless the individual or company operating the computer designates it as such. Here "the zone of privacy analysis focuses on the location of the information and governmental action."[8] In this sense, we consider necessary to examine the two most relevant

[5] U.S. Const. amend. IV.
[6] Katz v. United States, 389 US 347 (1967). This "search" case stated the basis for today's privacy doctrine which current courts' decisions follow (reasoned expectation of privacy). Thus, this decision indicated that government agents had to obtain a court order to place phone wiretaps.
[7] See supra note 4.
[8] See supra note 4.

circumstances to privacy concerns on electronic communications, specifically electronic mails:

> The technology has two characteristics directly relevant to privacy concerns. One deals with the use of electronic communications facilities and transmissions. E-mail issues thus involve questions of under what circumstances an individual or government entity can intercept the transmission itself. These issues are parallel to ordinary communications law questions and present no unique problems under modern law. The second characteristic, however, concerns the fact that E-mail messages are routinely stored under the control of private entities (for example, service providers, employers) and forwarded on to third parties by the recipient. Both characteristics reflect on to what extent the stored messages are private and against whom the privacy protection extends.[9]

In the case of **e-mail information in transit**, the constitutional frame of reference basically focuses on the degree of control (security) and the ability to exclude others from intercepting that information. This means that the conduct of the individual claiming privacy in the transmission of the electronic communication is important to state whether or not he had an objective expectation of privacy and whether that reliance was reasonable given the system in which the electronic communication was made. Furthermore, courts do not find a reasonable expectation of privacy from the mere use of a communication system. One the contrary, if the communication system is demonstrably insecure, then a warrant less interception may not be protected by the constitutional provision.

In addition, **stored e-mail messages** are also protected from governmental acquisition or intrusion under the Fourth Amendment restrictions on access.

[9] See supra note 4 at 8-76.

In Maxwell v. United States,[10] a court had to decide whether or not a defendant who had e-mail messages stored in a computer of an Internet Service Provider (ISP), America Online, indeed had a reasonable expectation of privacy. First, the lower court indicated that he did not meet the threshold requirements of showing a reasonable expectation of privacy (the precautions taken to preserve privacy), but though that there may have been a subjective expectation of privacy. An example of the latter could be "precautions such as making a phone call from an enclosed telephone booth, indicating the caller's intent to keep the conversation private, even though the caller uses a public phone booth and it is visible to the public."[11] On the other hand, the appellate court disagreed, concluding that, at least as to messages stored in the ISP computers, indeed a reasonable expectation of privacy existed under the constitution and it could be protected. In this sense, the court stated:

> We agree that appellant well may have forfeited his right to privacy to any e-mail transmissions that were downloaded from the computer by another subscriber or removed by a private individual from the on-line service. However…appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers…which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that appellant's computer transmissions would be received by anyone other than the intended recipients.[12]

[10] Maxwell v. United States, 42 MJ 568 (Ct. Military App. 1995).
[11] Katz, 389 U.S. at 353.
[12] Supra note 10, at 576.

Here the court made distinctions in terms of the degree of control that this person supposedly had regarding who can access and who received the messages, that is, in order to determine or establish the legitimacy of the expectations of privacy.

Once again, it is stated that the Fourth Amendment explicitly provides individuals the right to be secure from unreasonable searches and seizures. In other words, the founders of the Constitution intended that it be applied and construed in a flexible manner with the ability to adapt to changing circumstances.[13] However, the Constitution did not cover new technologies that could arise, not been able to foresee the several legal problems that could appear as a result of these technological improvements. Because of the fact that new technology presented new challenges at the time of determining whether or not a reasonable expectation of privacy existed, there was a clear effort to update the existing law with the enactment of the Electronic Communications Privacy Act of 1986.

B. The Electronic Communications Privacy Act of 1986.

For almost twenty years after its enactment, Title III of the Omnibus Crime Control and Safe Act of 1968[14] remained the only codified protection against invasions of privacy for oral and wire communications, regulating government surveillance of these communications and establishing restrictions on their activities. With the advent of cellular telephones, computer-to-computer transmissions, and electronic mail systems, technology outpaced Title III statutory protections against illegal federal interference and surveillance of communications, leaving the existing law "hopelessly out of date."[15] One of the main issues regarding these new technologies was that it was not always easy to determine whether or not a reasonable

[13] Johnny Gilman, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications,* 9 COMMLAW CONSPECTUS 111 (2001).
[14] 42 U.S.C. § 3789d, also called The Federal Wiretap Law.
[15] Michelle Skatoff-Gee, *Changing Technologies and the Expectation of Privacy: A Modern Dilemma,* 28 LOY. U. CHI. L.J. 189 (1996).

expectation of privacy existed, that is, a clear and objective expectation that the individual took the necessary security measures to assure his privacy within the use of new electronic communication methods such as "in transit" or "stored" emails. In an effort to update the existing law and keep pace with changing technology, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to amend Title III.[16] The ECPA consists of two parts, Title I and Title II, codified in chapters 119[17] and 121,[18] respectively, of Title 18 (Crimes and Criminal Procedure) of the United States Code ("U.S.C.").

As indicated above, Title I of the ECPA amended Title III of the Omnibus Crime Control and Safe Street Act by making the unauthorized interception of electronic communications illegal.[19] In other words, the purpose of this amendment was to modify privacy protections so that such protections (against government illegal interception during criminal investigations) might be modernized relative to technological advancements.[20] Congress also updated the existing act by adding "electronic communications to the type of communications which could be legally intercepted in criminal investigations.[21] Regarding these different types of communication covered by the act, we should take into consideration that "oral communication," remains the only type of communication that "explicitly" requires an expectation of privacy.[22]

---

[16] Id.
[17] *See* 18 U.S.C. § 2511(1994*),* for chapter 119 (Wire and Electronic Communications Interception and Interception of Oral Communications).
[18] *See* 18 U.S.C. § 2701 (1994), for chapter 121 (Stored Wire and Electronic Communications and Transactional Records Access). See also EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 168 (1996).
[19] 18 U.S.C. § 2511 (1994).
[20] David Hueneman, *Privacy on Federal Civilian Computer Networks: A Fourth Amendment Analysis of the Federal Intrusion Detection Network,* 18 J. MARSHALL J. COMPUTER & INFO. L. 1049 (2000).
[21] Id.
[22] Compare 18 U.S.C. § 2510 (2) (1994) (defining oral communication) with 18 U.S.C. 2510 (1) (1994) (defining wire communication) and 18 U.S.C. 2510 (12) (1994) (defining electronic communication).

Title I of the ECPA covers Fourth Amendment principles and include a provision supporting the "plain view doctrine". Protected communications that are revealed to the public lose their privacy expectations and therefore lose ECPA protection.[23] For example, a university that provides e-mail service to all of its students cannot intercept and access its students' messages because they hold a reasonable expectation of privacy in the transmission by using a password to access and secure their mail, both of them, the one that sends and the one that receives the message.[24] However, if the university sends an electronic mail message to all students, the university lacks any expectation of privacy in the transmissions and thus lacks ECPA protection.[25]

Furthermore, Title I indicates that in regard to e-mail accounts violations, any government employee who commits either of the following two actions without a court order violates the ECPA.[26] First, a person acts in violation of the ECPA if that person intentionally "intercepts" or endeavors to "intercept" any "electronic communication" while in transmission.[27] Second, a person acts in violation of the ECPA if that person intentionally uses or discloses or endeavors to use or disclose the "contents"[28] of any "electronic communication" while knowing or having reason to know that the information was obtained through the interception of an "electronic communication."[29] It's important to mention that both of these violations can occur only after an unauthorized interception.

---

[23] See 18 U.S.C. § 2510 (2) (1994).
[24] Michelle Skatoff-Gee, *Changing Technologies and the Expectation of Privacy: A Modern Dilemma,* 28 LOY. U. CHI. L.J. 189 (1996).
[25] Id. (no privacy interest for the content of an electronic mail transmission).
[26] EDWARD A. CAVAZOS & GAVINO MORIN, CYBERSPACE AND THE LAW 168 (1996).
[27] See 18 U.S.C. § 2511 (1) (a) – (b) (1994).
[28] Section 2510 (8) defines "contents" as "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510 (1994).
[29] See 18 U.S.C. § 2511 (1) (c) – (d) (1994).

While the ECPA makes it illegal for any person, including a system operator, to intercept or disclose an e-mail communication to anyone other that the addressee or intended recipient of such communication,[30] the Act does not prohibit a system operator from disclosing the contents of a communication to a law enforcement agency in any of four situations. First, a system operator may divulge the contents of a communication if authorized under section 2511 (2) (a) or 2517.[31] Second, a system operator may divulge the contents of a communication with the lawful consent of either the sender or the intended recipient of such communication.[32] Third, a system operator may divulge the contents of a communication to whomever it is necessary to forward the communication to its destination.[33] Finally, a system operator may also divulge the "contents" of an "inadvertently" obtained communication that appears to pertain to the commission of a crime, but only to a law enforcement agency.[34]

When the government performs an authorized interception or surveillance on a particular system, the ECPA places specific restrictions on a system operator. The Act clearly expresses that "no provider of an electronic communication service or any of its employees can disclose the existence of any interception, surveillance, or disclose the device used to accomplish the interception or surveillance, unless required to by the legal process.[35] Furthermore, an authorized disclosure may take place only after the prior notification to the Attorney General or to the principal prosecuting attorney.

[30] Section 2511 (3) (a) states that "an electronic communication service to the public shall not intentionally divulge the contents of any communication…while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication…" 18 U. S. C. § 2511 (4) (1994).
[31] See 18 U.S.C. § 2511 (2) (a) (1994). See also section 2517, "Authorization for disclosure and use of intercepted wire, oral, or electronic communications." 18 U.S.C. § 2517 (1994).
[32] 18 U.S.C. § 2511 (3) (b) (ii) (1994).
[33] 18 U.S.C. § 2511 (3) (b) (iii) (1994).
[34] 18 U.S.C. § 2511 (3) (b) (iv) (1994).
[35] See 18 U.S.C. § 2510 (15) (1994).

Any unauthorized disclosure renders the "electronic communication service" or particular employee liable for civil damages.[36]

In addition, the ECPA indicates that a person can lawfully "intercept" an "electronic communication", when such person is a party to the communication or when one of the parties to the communication gave prior consent to such interception. Also a person can lawfully "intercept" or access an "electronic communication" made through an "electronic communication system"[37] that is configured so that such communication is readily accessible to the general public.[38]

Although the ECPA protects e-mails and other forms of "electronic communication" from **private interception**, the law fails to provide "electronic communication" the same protection from **government interception** that a "wire" or "oral" communication could receive. First, an "electronic communication" may be intercepted for any federal felony whereas a "wire" or "oral" communication may be intercepted for only a handful of enumerated offenses.[39] Second, an application to a federal judge for a court "intercept" order to obtain an "electronic communication" may be approved by the Attorney General, any U.S. Attorney, or any authorized Assistant Attorney General or Assistant U.S. Attorney.[40] In contrast, an application to a federal judge for a court "intercept" order to obtain a "wire" or "oral" communication may only be approved by specifically designated attorneys in the Criminal Division of the U.S. Attorney's Office located in Washington, D.C.[41] Third, an "electronic communication" may be suppressed only through the judicially created

---

[36] Id.
[37] Section 2510 (14) defines an "electronic communication system" as "any wire, radio, electromagnetic, photo electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510 (14) (1994). A clear example of this is the Internet Service Provider or "ISP".
[38] 18 U.S.C. § 2511 (2) (g) (i) (1994).
[39] See 18 U.S.C. § 2516 (1994).
[40] Id.
[41] Id.

"exclusionary rule" when a constitutional violation occurs,[42] whereas a "wire" or "oral" communication may be suppressed through the statutorily created "exclusionary rule" whenever the violation of a "central" or functional provision of the ECPA occurs.[43] These three differences represent a serious threat to the use of new technologies, because citizens will stop using these and replace them with older communication technologies that are safer and provide more privacy protection from government interception. A problem even worse to the foregoing is government access to a stored "electronic communication."

III. The ECPA does not offer enough privacy protection for citizens regarding their stored electronic communications.

A. The Access to and Disclosure of Stored Electronic Communications.

Unlike Title I of the ECPA that deals with "Wire and Electronic Communications Interception and Interception of Oral Communications", Title II of the same act regulates "Stored Wire and Electronic Communications and Transactional Records Access." It makes illegal the unauthorized access to stored wire and electronic communications.[44] Under Title II, government agents authorized to access stored communications must retrieve the information from the service provider. In regard to the unauthorized "access" of a stored private e-mail communication, the ECPA has a dual purpose.[45] First, the ECPA outlaws most

[42] Despite it is not statutorily created, the "exclusionary rule" in "electronic communication" matters currently represents the most effective means of enforcing the Fourth Amendment. As a result, it bars the use in federal or state court criminal proceedings of evidence that a federal or state government obtains in violation of the Fourth Amendment.
[43] See 18 U.S.C. § 2515 (1994).
[44] 18 U.S.C. § 2701-2711 (1994). Section 2701 (a) provides the following:
Whoever – (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided…
[45] Robert S. Steere, Note, *Keeping "Private E-mail" Private*, 33 VAL. U. L. REV. 231 (1998).

unauthorized private access.[46] Second, the ECPA provides prerequisites for government access.[47] A government entity may require an "electronic communication service" to disclose the contents of an "electronic communication" held in "electronic storage" for 180 days or less only pursuant to a warrant supported by probable cause.[48] On the contrary, a government entity may require an "electronic communication service" to disclose the contents of an "electronic communication" held in "electronic storage" for more than 180 days pursuant to a warrant, administrative subpoena, or court order.[49] Unlike a warrant supported by probable cause, an administrative subpoena requires no factual basis and a court order requires a mere offering of "specific and articulable" facts showing reasonable grounds to believe that the contents of an "electronic communication" are relevant to an ongoing criminal investigation.[50] Thus, the ECPA provides less protection for an "electronic communication" kept in "electronic storage", especially when compared to a "wire communication" kept in the same storage method.

Although the ECPA provides some protection for e-mail and other forms of "electronic communication" kept in electronic storage, the law does not provide an "electronic communication" the same level of protection from government access that a "wire communication" receives. Government access to a stored "wire communication" requires an intercept order,[51] whereas the government can access a stored "electronic communication" through a warrant, a subpoena, or court order.[52] In other words a stored "wire communication" has strict protection in the Title I court "intercept" order, whereas an "electronic communication" receives the less protection

[46] Id.
[47] Id.
[48] 18 U.S.C. § 2703 (a) (1994).
[49] 18 U.S.C. § 2703 (a) – (d).
[50] 18 U.S.C. § 2704 (d).
[51] See 18 U.S.C. §§ 2516, 2218 (1994).
[52] 18 U.S.C. § 2701 (a) (1) (1994).

found in Title II. The foregoing shows us the degree of threat that this gaps and inequalities in the current act represent to people's privacy rights, specifically regarding unauthorized and abusive **access** to stored "electronic communications."

Regarding the "disclosure" of a stored "electronic communication" in the form of a private e-mail, the ECPA proscribes a person or entity providing an "electronic communication service" to the public from knowingly divulging to anyone the "contents" of a communication while in "electronic storage:"[53] However, an "electronic communication service" may divulge the "contents" to an addressee or intended recipient of such communication[54] or to a person whose facilities are used to forward a communication to its intended destination.[55] Likewise, an "electronic communication service" may divulge the contents of an "electronic communication" that may be necessarily incident to the rendition of that service, such as to protect the property of the service[56] or as otherwise authorized in other sections of the ECPA.[57] Finally, if the "electronic communication service" inadvertently obtains the contents of an "electronic communication" that appear to pertain to the commission of a crime, then the service provider may divulge the contents to the government.[58]

These provisions indicated above clearly show us that stored "electronic communications" are easier to obtain by government officials than "wire communications", a direct consequence of lesser protections explicitly enacted by Congress through the ECPA.

---

[53] See 18 U.S.C. § 2702 (1994).
[54] 18 U.S.C. § 2702 (b) (1).
[55] 18 U.S.C. § 2702 (b) (4).
[56] 18 U.S.C. § 2702 (b) (5) ("as may be necessarily incident to the rendition of such service or to the protection of the rights or property of the provider of that service").
[57] 18 U.S.C. § 2702 (b) (2) ("as otherwise authorized in section 2517, 2511 (2) (a), or 2703 of this title").
[58] 18 U.S.C. § 2702 (b) (6).

B. Why ECPA fails to provide enough protection to stored electronic communications and proposals to modify this.

At the beginning, the main interest of Congress was to create through the enactment of the ECPA a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.[59]

Nowadays, the ECPA fails to provide enough privacy protections to "electronic communications" for several reasons. These include gaps in this current statutory framework, such as ambiguities at the time of interpretation of several definitions, as well as lack of up to date provisions regulating new and always changing communication methods. Thus, Congress must modify the ECPA and clarify the distinction between an "electronic communication" in "transit" as opposed to an "electronic communication" held in "electronic storage," in order to protect a citizen's right of privacy, not allowing law enforcement agencies to avoid the more stringent requirements for a court "intercept" order. If law enforcement agencies have the ability to sidestep the court "intercept" order for an "electronic communication," then citizens who communicate by "electronic communication" do not receive the same protection from overzealous law enforcement agents as citizens who communicate by "wire communication" or "oral communication."[60]

Also "electronic communication" in storage for any length of time should only be acquirable upon federal[61] or state warrant, and not determine the requirement to acquire them by a specific time term because privacy interests are always present. Thus, as stated before, the public has a reasonable expectation of privacy with regard to electronic data, like e-mail, regardless for instance, of whether ISP employees can access such files for maintenance of the system and some other duties. This analysis

[59] Robert S. Steere, Note, *Keeping "Private E-mail" Private*, 33 VAL. U. L. REV. 231 (1998).
[60] Id.
[61] This federal warrant must be issued under the Federal Rules of Criminal Procedure.

indicate that Congress should add to the ECPA provisions in this sense, so that time limits do not affect people's expectation of privacy and statutory requirements for surveillance and access of stored "electronic communications" be the same as those for stored "wire communications."

Regarding current investigation tools to conduct electronic surveillance of electronic mail messages and other online communications that could be related to criminal acts, such as terrorism, espionage, information warfare, child pornography, serious fraud, and other felonies, we consider necessary to mention the existence of the **Carnivore System**[62], which was known for the first time in the year 2000. In general terms, this FBI's Internet search tool is designed to collect from any ISP system "electronic communications" based on e-mail addresses, key words, or Internet protocol addresses.[63] The problem with this new search tool is that the current legal framework, that is, the ECPA, do not provide up to date provisions to protect electronic communications as a whole. Thus, the Carnivore can scan millions of e-mails in second, having access to intercepting all type of information, both authorized and unauthorized.[64] A lot of questions arise concerning who controls Carnivore so that it strictly complies with court's order or warrants indicating specific searches and surveillance and not the entire ISP system[65], obviously having access to all real-time and stored e-mail transmissions, addresses, Internet Protocol packets (IP) customer's private information and the unimaginable; in other words, who oversees the FBI in order to assure that government agents only make lawful use of the

[62] See U.S. Department of Justice Carnivore System's Review: Draft Report: Independent Technical Review of the Carnivore System at http://cryptome.org/carnivore-rev.htm.
[63] Maricela Segura, *Is Carnivore Devouring your Privacy?,* 75 S. CAL. L. REV. 231 (2001). (Also called "the FBI's new Internet wiretapping system").
[64] See Illinois Institute of Technology Research Center Report for further information on the Carnivore System: Independent Review of the Carnivore System: Draft Report 1-1 (Nov. 17, 2000), at http://www.cdt.org/security/carnivore/00111/draftreport.pdf
[65] Johnny Gilman, *Carnivore: The Uneasy Relationship Between the Fourth Amendment and Electronic Surveillance of Internet Communications,* 9 COMMLAW CONSPECTUS 111 (2001).

system? Congress should also oblige the government to include an auditing system within the Carnivore program in order to ensure that government agents (FBI) are not overstepping the bounds of the search outlined in a court order.[66] The existence of this surveillance engine makes us think about how broad is this tool's scope, being able to scan, search and survey infinite amounts of files, personal information, emails from all customers of an ISP, for instance, Microsoft's "Hotmail" accounts, which are popular not only in the United States, but in a worldwide level, probably violating not only U.S. citizen's privacy rights, but from people all over the world.

Taking into consideration this current investigation tool and its broad applications, we can realize that there are specific deficiencies in the ECPA protection of "electronic communications" regarding government restrictions and previous requirements to access this type of communication. For instance, the formalistic distinctions between wire and electronic communication and between "new" and "old" email[67] has created a legal framework that is "meaningless" with respect to the public's expectation of privacy.[68] At the end, this legal framework shows the enormous tension between upholding a citizen's right to privacy and promoting technologies that contribute to law enforcement efforts.

IV. Conclusion.

The inefficiency of The Electronic Communications Privacy Act of 1986 to protect citizen's privacy rights on stored "electronic communication" is a fact. It fails to provide enough protection to these new communication methods, which nowadays more and more individuals are using.

---

[66] Id.
[67] This criterion for classifying e-mails is based on the time term of less or more than 180 days, as established by the ECPA, determining with this the statutory requirement (warrant, subpoena, or court order) needed before acquiring access and pursue surveillance of electronic communications.
[68] Robert S. Steere, Note, *Keeping "Private E-mail" Private*, 33 VAL. U. L. REV. 231 (1998).

It is clear that amendments to the current ECPA are needed in order to guarantee citizen's expectation of privacy in stored "electronic communications", regulating and restricting government access to these stored "e-communications", protecting with these intrinsic and inalienable rights that the framers of the Constitution stated in the Fourth Amendment, preserving privacy principles and maintaining its effectiveness over multiple intrusions from individuals and government agents.

In addition, the statutory framework must be also amended to specifically provide "electronic communications" with protections similar to those afforded to "oral" and "wire" communications. With these amendments citizens will be secure in knowing that their communication is free from government interception from the time they speak or type until the time the recipient hears or reads the "electronic communication."