Oscar Wilde once observed, “[i]t is only the modern that ever becomes old fashioned.”¹ Nowhere is this paradox more evident than in the area of advanced technology. The pursuit of new technology has been the hallmark of western civilization since the dawn of the industrial era. Simply put, as technology develops, older equipment becomes obsolete. The renowned economist Joseph Schumpeter coined this process, naming it “creative destruction.”² Additionally, the lives of average people have been undeniably affected by the adoption of new technologies – technologies, such as the Internet that allow access to near infinite stores of information from almost any location.³ While fear of technology has spawned a number of “doomsday-type” action movies,⁶ society has recognized the gains attendant to technology and has become more comfortable accepting new technology. The legal system, however, does not adapt so quickly. It has been said that “the wheels of justice grind slow, but exceedingly fine.”⁷ Whether law is created through the judicial or legislative process, it is rare that it

“Laws tend to be written to address the particular technologies of the day, and as that technology becomes obsolete, the laws related to that technology become obsolete too.”

Joseph Schumpeter coined this process, naming it “creative destruction.”² As new innovations are adopted, older technologies are swept aside, never to be used again.³ In recent decades, our society has become more apt to embrace changes in technology. Businesses in the United States have been able to increase worker productivity at an almost unthinkable rate by incorporating the latest technology.⁴ Additionally, the lives of average people have been undeniably affected by the adoption of new technologies – technologies, such as the Internet that allow access to near infinite stores of information from almost any location.⁵ While fear of technology has spawned a number of “doomsday-type” action movies,⁶ society has recognized the gains attendant to technology and has become more comfortable accepting new technology. The legal system, however, does not adapt so quickly. It has been said that “the wheels of justice grind slow, but exceedingly fine.”⁷ Whether law is created through the judicial or legislative process, it is rare that it
can be created rapidly. In recent memory, only the anti-terror laws created in the wake of 9/11 and the corporate laws created after the Enron and WorldCom scandals were enacted with any rapidity. Most other laws have been forced to grind their way through the legal machine.

The legal system's inherent slowness can be a detriment to society when it comes to dealing with advanced technology. Laws tend to be written to address the particular technologies of the day. As that technology becomes obsolete, the laws related to that technology become obsolete too. The laws must be created anew to address the new technology specifically. Inevitably there will be a time lag between the obsolescence of the law relating to the old technology and the creation of law addressing the new technology. During this time lag, there is a significant opportunity for abuse. Thus, the question arises: how can the legal system reduce the amount of time between technology adoption and proper regulation?

This article will examine the obsolescence of laws through the lens of recent cases relating to “wiretapping laws” and propose the creation of laws that protect certain rights independent of technology. Recently, a number of courts have held that laws created in the mid-1980’s to protect communications do not apply to Internet-related communications, reasoning that the method of transmission falls outside the language of the statutes. As a result, e-mail and other forms of Internet-based communications are treated differently from older forms of communication such as telephone conversations. This article will propose a broad legislative solution with the aim of both extending protections to the new forms of communication and providing a framework for dealing with new forms of communications technology as they are developed. Though this specific solution will apply merely to the technology at issue, the same approach could be used to address other technologies that have not yet been created.

Section II will briefly lay out the development of the current wiretapping laws. Section III will illustrate the two-fold problem that the recent court cases have created. Finally, section IV will evaluate possible methods for protecting the newer forms of communication.

“... the advance in communications technology necessitated the enactment of laws protecting persons from invasions of privacy that were damaging to the invadee’s feelings.”

I. Background: The Evolution of the Wiretapping Laws and the Right to Privacy

Protecting privacy in communication is by no means a recent proposition. Communication via mail has been protected against unwanted searches since the 1870’s. In Ex Parte Jackson, the Supreme Court held that the Constitutional protections against unreasonable searches and seizures extend to peoples’ papers that have been closed against inspection. The Court further held that letters could be searched only after a warrant was procured, stating that “[n]o law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail.” This protection of mail was later codified by Congress and remains in force today.

Though the telephone was invented in 1876, it was not given protections similar to
those afforded postal mail until the mid 1960’s. This is shocking, as the information obtainable through telephone conversations can be much more private than that found in mail. The Senate Judiciary Committee observed:

[w]hen the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the “houses, papers, and effects” protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

Telephone conversations were first protected from surveillance by authorities on Constitutional grounds by the Supreme Court, and state courts created a form of the “invasion of privacy” tort to protect against surveillance by civilians.

A. The Right to Privacy: The Starting Point of the Wiretapping Law

The right to privacy has been developing in the U.S. since the late 19th Century. The idea of a “right to privacy” was first championed in one of the most famous law review and aptly named articles of all time, The Right to Privacy. Justices Louis Brandeis and Samuel Warren argued that the common law grows in order to better protect society. Thus, laws protecting against threat of injury as well as injuries to one’s reputation emanated from laws protecting against bodily injury. Brandeis and Warren believed that it was time for the law to grow again.

Brandeis and Warren stated that the advance in communications technology necessitated laws to protect against injurious invasions of privacy. After looking at a number of English common law cases, they drew the conclusion that courts could protect a person’s privacy. Thoughts, emotions, and sentiments expressed in writing or the arts could be prevented from publication by their respective author. Thus, by protecting a person’s right to privacy, courts are merely enforcing that individual’s rights. Brandeis and Warren then proposed a tort which would protect individual’s privacy to the extent that the individual kept their private life private. In situations involving wiretapping, state courts enacted this tort in the form of invasion of privacy.

B. Development of Tort of Invasion of Privacy for Unreasonable Intrusion.

Due to the unwillingness of federal courts to protect telephonic communication, the earliest protections came by way of state court tort adjudication. Following the publication of Brandeis and Warren’s article, state courts began to apply the doctrine the authors had proffered and essentially created the tort of “Invasion of Privacy.” As early as 1931, state courts held that wiretapping was a legally redressable invasion of privacy. The tort is currently recognized in almost all jurisdictions though the specifics of the tort and its application vary. Cases involving misappropriation of communication fall under the unreasonable intrusion strain of the tort. Although most state courts recognize wiretapping to be an invasion of privacy and generally agree to the basic scope of the tort, they differ on certain specifics. The courts agree that there must be an intrusion into a matter that is, and is entitled to be, private. Stated differently, for the protections to apply, the matter at issue must be of the type normally kept private. Pretrial testimony, police photography, and corporate records made public by law are among those matters not considered to be kept private. Furthermore, most actions or statements made in public are not considered private. Thus, the courts agree as to the broad application of the tort.

The courts diverge, however, when it comes to some of the specifics of the tort as it relates to wiretapping. Some courts have followed a more permissible standard, finding liability where a wire had been tapped but no one was listening and where the information found by way of wiretapping was not disclosed to third parties. Others require that there be evidence that the wrongly obtained information be disclosed to unauthorized persons.
though the courts agree in the broad strokes about invasion of privacy, the patchwork of different state law can render the tort difficult to pursue.

C. Creation of protections from governmental intrusion

Protections against wiretapping were enacted on a federal level decades after state tort protections appeared. The federal protections first emerged in Supreme Court adjudication as protections against government intrusions under the Fourth Amendment. When Congress codified these protections, they expanded them to protect citizens from both government and civilian actors.

1. Olmstead v. United States: The Court restricts search and seizure protections to the physical realm

In early decisions, the Supreme Court was initially skeptical of protections against wiretapping and refused to extend any protection similar to that afforded mail to telephone communication. For example, in Olmstead v. United States ("Olmstead") the defendants were convicted of conspiracy to violate the National Prohibition Act by importing alcohol. The conspiracy was discovered when federal agents tapped the phone lines of the conspirators. Finding that the Fourth Amendment protections against search and seizure covered only the physical realm, the Court held that the phone tapping was permissible. The Court stated:

[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.

Brandeis stated that the makers of the Constitution gave citizens the right to be left alone and, to protect this right, all unjustifiable government intrusions "must be deemed a violation of the Fourth Amendment." Thus, Brandeis called for Constitutional protections which would have extended beyond the realm of physical searches and seizures. Nevertheless, the majority held the day and found that wiretapping was not illegal. Brandeis' dissent was remarkably prescient, however, as Olmstead was not the end of the wiretapping debate.

2. Katz v. U.S.: The Supreme Court largely follows Brandeis' logic and extends protections to telephone conversations

The Court revisited wiretapping in Katz v. United States and chose to follow most of Brandeis' reasoning. In Katz, the petitioner had been convicted of making illegal wagers based on telephone conversations that he made in a public telephone booth that the FBI had wiretapped. The Court of Appeals for the
Ninth Circuit evaluated the case using a physical-realm focused Fourth Amendment examination. The Court of Appeals held that there was no violation of the Fourth Amendment because "there [had been] no physical entrance into the area occupied by the petitioner." The Supreme Court in *Katz* rejected the *Olmstead* Court's reasoning, stating that "the Fourth Amendment protects people, not places," and "wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures." The Court held that the government violated the privacy that the defendant justifiably relied upon through its electronic surveillance. The majority stated that whatever a person seeks to preserve as private may be protected by the Constitution. Further, the Court held that this privacy could only be invaded by the government after it has "advance authorization by a magistrate upon a showing of probable cause." However, the *Katz* Court refused to apply Brandeis' broad view regarding the right to be left alone. The majority held that, although the Constitution protected persons from government intrusion, a person's general right to privacy was an issue for individual states to decide, much like the protection of personal property.

3. The prohibitions against wiretapping were enacted in 1968, and then amended in 1986 after they had become obsolete

The year after the Supreme Court decided *Katz*, Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968 ("wiretapping laws"). This legislation responded to the *Katz* decision by creating a scheme under which the government could use wiretapping in law enforcement after receiving authorization from a judicial official. Protections from the law extended against both government and civilian actors. The 1968 wiretapping law, however, covered only oral communications carried over common telephone carriers. Congress recognized that the years following 1968 saw rapid changes in the communications industry. Many new technologies including electronic mail, cellular telephones, pagers, and video teleconferences were not considered in the 1968 law. Furthermore, with the breakup of the AT&T monopoly, many telephone calls were no longer carried by common carriers and did not fall within the scope of the wiretapping laws. The Senate observed that, though a first-class letter was afforded a high level of security, no comparable security existed for "new non-common carrier communication services." Therefore, after concluding that the present laws were "hopelessly out of date," Senator Patrick Leahy introduced legislation that would overhaul the wiretapping scheme.

The Electronic Communications Privacy Act of 1986 updated the wiretapping laws "in light of the dramatic changes in new computer and telecommunication technologies." It remains the primary protection of communications. Although amendments have been made over time, most
notably with the enacting of the Patriot Act, the structure of the wiretapping laws has not changed since 1986.\textsuperscript{80}  

The current wiretapping scheme is divided into two main sections: Title I and Title II.\textsuperscript{81} Title I governs the interception of wire and electronic communications.\textsuperscript{82} Title II governs stored communications and transactional records.\textsuperscript{83} Title I expands the provisions of the 1968 law to cover different forms of oral and aural communication.\textsuperscript{84} This title prohibits the interception of wire, oral, or electronic communication, as well as the disclosure of information thereby obtained, unless the interception was authorized by court order.\textsuperscript{85} It broadly defines “intercept” to include “the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.”\textsuperscript{86} Further, this title broadly defines “oral communication” as including any oral communication where a person has a reasonable expectation that the communication will not be intercepted.\textsuperscript{87} Thus, Congress expanded the law to include new forms of technology.

Whereas Title I was a mere expansion of old laws, Title II was a completely new legal scheme.\textsuperscript{88} Recognizing that a whole host of new communications options had emerged in what we now know as the Internet, Title II was Congress’ attempt to extend the same protections to these new mediums.\textsuperscript{89} The statute outlaws the unauthorized access to “facilities through which electronic communications service is provided.”\textsuperscript{90} In other words, Title II protects servers which are used for transmission of e-mails from some unauthorized intrusions.\textsuperscript{91} However, it includes an exception that allows service providers to access the stored communications.\textsuperscript{92} Thus, service providers can look into the e-mails stored on their servers without violating the statute.\textsuperscript{93}

\section*{D. Recent court rulings show that the law has again become obsolete with respect to wiretapping prohibitions}

Despite the best efforts of Congress to pass comprehensive wiretapping laws, recent court rulings have shown the law to be obsolete and in need of repair. The First, Third, Fifth, Ninth, and Eleventh Circuit Courts of Appeal have found areas in which the current wiretapping laws do not protect communications.\textsuperscript{94} The Fifth Circuit was the first to decide that the wiretapping laws did not apply to a new form of communication.\textsuperscript{95} In \textit{Steven Jackson Games, Inc. v. United States Secret Service}, the Secret Service seized a computer which operated a Bulletin Board Service.\textsuperscript{96} Subsequently the Secret Service read and deleted a number of e-mails which were stored on the same computer.\textsuperscript{97} The \textit{Steven Jackson Games} court found that the Secret Service’s actions did not violate the wiretapping laws because the e-mails did not constitute protected electronic communications.\textsuperscript{98} The \textit{Steven Jackson Games} court, following a plain-text reading of the wiretapping laws, stated that:

\begin{quote}
[The E-mail at issue was in “electronic storage.” Congress’ use of the word “transfer” in the definition of “electronic communication,” and its omission in that definition of the phrase “any electronic storage of such communication” (part of the definition of the definition of “wire communication”) reflects that Congress did not intend for “intercept” to apply to “electronic communications” when those communications are in “electronic storage.”]
\end{quote}

\textsuperscript{99} Thus, the \textit{Steven Jackson Games} court held that due to Congress’ formulation of the wiretapping laws, e-mail stored on a computer is not protected communication.

Similarly, in \textit{Konop v. Hawaiian Airlines, Inc.}, (“\textit{Konop}”) the Ninth Circuit held that an “interception” can only occur during the transmission of electronic data.\textsuperscript{100} In \textit{Konop}, a pilot for Hawaiian Airlines created a website critical of his employer, keeping the website secure by allowing only authorized users with a username and password to access it.\textsuperscript{101} Subsequently, a vice president of the airline accessed the website using another employee’s username and password.\textsuperscript{102} The court held that the vice president’s actions did not constitute an “interception” under the Stored
Communications Act (“SCA”).103 Adopting the reasoning that it had stated in United States v. Smith104 – that communications covered by the SCA are afforded less protections than those covered under the Wiretap Act – the court held “that for a website to be intercepted in violation of the [Wiretap laws], it must be acquired during transmission, not while it is in electronic storage.”105 Thus, the court held that an “interception” had not occurred because the data had not been acquired during the transmission.106

The reasoning of the Fifth and Ninth Circuits has been adopted by the Eleventh and Third circuits.107 In United States v. Steiger, the Eleventh Circuit observed that:

...very few seizures of electronic communications from computers will constitute “interceptions.” There is only a narrow window during which an E-mail interception may occur – the seconds or mili-seconds (sic) before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used ... interception of E-mail within the prohibition of the Wiretap Act is virtually impossible.108

Similarly in Fraser v. Nationwide Mutual Insurance Company, the Third Circuit noted that “[w]hile Congress’s definition of “intercept” does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched.”109

Most recently, the First Circuit adopted the Fifth and Ninth Circuit’s definition of interception.110 In U.S. v. Councilman, a book dealer provided his clients with e-mail accounts.111 The dealer then installed a program on his server that sent copies of any client e-mail from Amazon.com to his mailbox.112 After adopting the narrow reading of the SCA, the court observed that “the language [of the wiretapping laws] may be out of step with the technological realities of computer crimes.”113 Further, the court stated “much of the [wiretap laws] protection may have been eviscerated by the realities of modern technology.”114 Judge Lipez, dissenting, stated his belief that the wiretapping laws were unclear on the issue at hand, but that congressional intent clearly expressed a desire to protect e-mails.115

E. Legislative Responses to the recent Court Rulings

Understandably, the recent rulings by the Circuit Courts have led to a public outcry.116 A reporter for The New York Times observed:

America’s right to privacy will be seriously eroded if e-mail is not protected by wiretap laws. The implications of this erosion extend beyond the commercial realm... Congress ought to update the law to make it clear that e-mail is entitled to the same protections as a phone call.117

On July 22, 2004, barely a month after the First Circuit’s ruling in Councilman, two bills were submitted to Congress that sought to
correct the deficiencies in the wiretapping laws. House Resolution 4956, proposed by Congressman Inslee, would remedy the problem by expanding the definition of “interception” to include “the acquisition of the contents of the communication through the use of any electronic, mechanical or other device, at any point between the point of origin and the point when it is made available to the recipient.” Similarly, House Resolution 4977, introduced by Congressman Nadler, would remedy the problem by expanding the definition of “electronic communication” to include “any temporary, intermediate storage of that communication incidental to the communication thereof.” Thus, both bills would amend the wiretapping laws and protect Internet-based communications that are in temporary storage on a server by either expanding the definition of interception or the definition of electronic communications. Further, both bills would limit the protections granted to service providers under the SCA by forcing the providers to show that they accessed the e-mails for the purpose of providing their service or protecting the rights of their customers or themselves.

II. The Cases Raise a Two-fold Problem: How Can We Protect Internet-based Communications and Ensure that Communications Protections Do Not Become Obsolete?

The wiretapping adjudications raise a two-fold problem. First, the cases illustrate that Internet-based communications are not protected by the current wiretapping laws. Second, the cases illustrate the broader problem of legal obsolescence in the technological area. The solution proposed in Section IV would address both aspects of the problem through the creation of laws independent of technology and thus independent of the obsolescence problem.

A. The Immediate Problem: Protecting Internet Communications

Though the wiretapping adjudication has focused for the most part on what could be termed “traditional Internet-based communications,” the cases have broader implications. The expanding use of Internet-based communications, such as Voice over Internet Protocol (“VoIP”), brings voice and video communications within the scope of the e-mail case-law. Thus, under this reading of the case-law, virtually all Internet-based communications can be intercepted without legal recourse.

Internet-based communications are communications sent from one networked computer to another. Most Internet-based communications function similar to e-mail messages sent from computer via Simple Message Transfer Protocol (SMTP), the predominate e-mail protocol. Under SMTP, the messages are not sent directly from one computer to the next; rather, the messages are sent through a number of intermediate servers before arriving at their final destination. The messages are generally sent from the creating computer to the nearest server. That server then finds where the message should be sent and forwards it. The message is passed from server to server until it reaches its final destination. Prior to sending the message on to the next server, the servers often store a temporary copy of the message. This procedure allows the server to route messages more efficiently and handle for higher than normal traffic volumes. Because it sends messages from server to server and does not require a direct connection, the Internet is able to send messages between two different computers through a number of alternative paths.

Due to this prolonged process of transmission, the Internet is a redundant communications medium, wherein messages pass through many intermediate servers before arriving at their final destination. The courts, however, have held that as messages pass through the intermediate servers, they are not protected against unauthorized interception and dissemination. The courts have consistently held that messages are not protected when they are stored on intermediate computers, even though the storage is incident to their transmission. Rather, messages must be intercepted while in transmission for a violation of the wiretapping laws to occur.
While the ever increasing reliance upon e-mail and other text based messaging systems would make these holdings troubling enough, the rapid increase in other forms of Internet-based communications has only worsened the situation. In recent years, Internet communications have grown to include telephone and video services. Illustrating the rapid adoption of these technologies, one provider, Vonage, saw its subscriber base quadruple in 2004. Using this technology, commonly known as VoIP, a number of companies, including Vonage and Comcast, allow residential and business customers to communicate telephonically without using a traditional telephone line.

VoIP systems use communications protocols similar to those of more traditional Internet communications techniques such as e-mail and other text messaging. Thus the security of a company’s entire communications system, both text-based and voice-based, could be compromised; and, under current wiretapping law, these companies would have no apparent legal recourse. According to the federal courts current construction of the wiretapping laws, communications can only be intercepted while in transmission. Consequently, the law would not apply to any portions of the communication that are stored on the servers, even if the storage was incident to the transmission. These communications could be read by the owners of any server that they happened to pass through. Such a result clearly runs counter to the stated intent of Congress and is both inequitable and unjust.

B. The Long-term Problem: Dealing with Legal Obsolescence

Though the wiretapping law’s failure to protect Internet-based communications is a problem in itself, it is also illustrative of a bigger issue that will continue to plague our technology based society for the foreseeable future. Many laws are written with a specific technology in mind and they are thus tailored to fit the problems native to that technology. Over time, however, in a vibrant society such as ours, Schumpeter’s law of creative destruction will render the specified technology obsolete. The technology that rendered the first technology obsolete, however, will not be protected by our legal system. The law that protected the old technology will likely be adapted to its inner workings. Thus, the workings of the new technology will most likely set it outside of the four corners of the existing law. The new technology will render obsolete not only the old technology but also the related law.

This process of legal obsolescence has been illustrated by the evolution of the wiretapping laws. The first wiretapping laws were created in the late 1960’s and focused on the nature of the telephone industry. At that time the monopolistic system “Ma Bell” was in place, and thus, the law focused purely on telephone conversations carried over the common carrier. Less than twenty years later, the break up of Ma Bell and the advent of new technology necessitated a complete rewriting of the wiretapping laws. However, even this rewrite did not offer communications protections for very long as courts found that the wiretapping laws did not cover certain electronic communications. Thus, a mere
eight years after the law had been modified, it was already becoming obsolete. Since 1994, the obsolescence of the law has continued with each Circuit Court decision; no one has stopped the decline.

On a broad level, the obsolescence of laws poses significant problems for our legal system and our society as a whole. As the Circuit Court decisions illustrate, judges are often unwilling to act beyond the legislative mandate in areas of criminal law. Thus, in the wiretapping arena, the same communication might be sent over two mediums, it would appear identical to the sender and receiver, but it would receive very different legal treatment. This differing legal treatment adds uncertainty to the marketplace of technology. As business and consumers discover that their use of new technology may not be given the same protections as the old, they will alter their behavior accordingly by not using the new technology to its full extent. This reduced use of the new technology will lead to the loss of the efficiency that the new technology would provide. To prevent this loss of efficiency, and the resulting damage to the economy and society as a whole, the law must find a way to deal with new technology as it develops. By reducing the lag between technology adoption and legal administration of the technology, the law will encourage earlier adoption of new technology and the attendant benefits to society.

III. The Solution
The solutions have been divided into two categories: narrow and broad solutions. The narrow solutions seek to extend the protection of the wiretapping law to Internet-based communication and thereby solve the pressing problem. The broad solutions seek to address both the immediate problem of Internet-based communications, as well as put in place a framework for the courts to handle issues that arise from new communications technology. For the reasons explained below, a broad legislative solution would offer the best answer.

A. The Narrow Judicial Solution
A narrow solution crafted by the judiciary would look beyond the plain language of the wiretapping law and expand the law to conform to the intent of Congress. Such an approach was offered by Judge Lipez in his dissenting opinion in Councilman. In Councilman, Judge Lipez noted that “the legislative history [of the wiretapping laws] demonstrates that Congress was deeply concerned with the emerging threats to privacy and the failure of existing legal protections to cope with these threats.” Congress intended to protect the privacy of e-mail, because it did not perceive any Constitutional protections existed for it. Judge Lipez stated that the plain language of the statute does not address whether storage incident to transmission of e-mail is considered a transmission which can be intercepted. Further, Judge Lipez declared that the majority’s rationale was flawed, and he found “it inconceivable that Congress could have intended [that e-mails not be protected by the wiretapping laws] merely by omitting the term ‘electronic storage’ from its definition of ‘electronic communication.’” Thus, he would have held that e-mails could...
be intercepted because it was the purpose and intent of Congress to protect communications, including electronic communications.\textsuperscript{161}

Judge Lipez’s approach would solve the problem of protecting Internet communications by looking to congressional intent to fill in gaps in the wiretapping laws. However, it appears unlikely that his approach would be uniformly adopted as five separate Circuit Courts of Appeal have rejected it.\textsuperscript{162} Judge Lipez makes a very persuasive case for looking beyond the text of the wiretapping laws to find protections for Internet communications. Nevertheless, as previously illustrated, most of the courts that have examined the problem have refused to go beyond the “four corners” of the law, insisting that Congress must cover its own bases.\textsuperscript{163}

A court following Judge Lipez’s approach would run counter to all previous circuit court adjudication. Therefore the best case scenario for this approach would be for a circuit split to develop, which might lead the Supreme Court to resolve the split in favor of using congressional intent to fill in the wiretapping law’s gaps. This scenario also seems very unlikely as courts have consistently chosen not to follow this route.\textsuperscript{164} In fact, the Ninth Circuit, which harbors an activist reputation,\textsuperscript{165} and the Fifth Circuit, whose reputation is decidedly conservative,\textsuperscript{166} have both rejected Judge Lipez’ logic.\textsuperscript{167} Thus, the narrow judicial solution is a perilous approach at best.

Additionally this approach would do nothing to protect new technologies. Judge Lipez’ approach could be used to protect e-mail and other Internet-based communication because Congress clearly intended to protect it. However, if a new technology which had never been discussed in Congress were at issue, this approach would not be helpful, because the judge would have no Congressional guidance at all. Thus the narrow judicial approach does nothing to address the broader problem of dealing with the obsolescence of laws.

B. The Narrow Legislative Solution

Legislation pending in the House of Representatives, if enacted, would extend the protections of the wiretap law to Internet communications.\textsuperscript{168} There are two bills pending, each of which would amend the wiretap law by expanding either the definition of “interception” or the definition of “electronic communication.”\textsuperscript{169} The plain language of the wiretapping laws would thus allow for protection from interception of e-mails and other Internet-based communications.\textsuperscript{170} In this way, as suggested by the Fraser court, Congress would finally cover its bases.\textsuperscript{171}

While the proposed legislation would resolve the narrow issue of protecting e-mail and other Internet-based communications from wiretapping, it would not help to protect communications proactively. Should the underlying technology change, Congress would then have to amend the law again to reflect the changes. Consequently, though this solution would solve today’s problem, it would do nothing to prevent the legal uncertainty that would accompany any future technological innovations.

C. The Broad Judicial Solution: The Institution of a Right to be Left Alone

A judicially imposed solution could create a framework that would protect communications, and thereby both protect existing Internet-based communications and provide guidance for protecting new forms of communications yet to be invented. Such a framework could be created using pre-existing Constitutional and tort concepts employing a minimum of two components: one grounded in the Fourth Amendment pertaining to Government intrusion and the other based on the tort of invasion of privacy.

1. Protections based on the Fourth Amendment to restrain government intrusion and tort law could protect communications in the civil realm through an expanded use of invasion of privacy doctrine.

A judicial doctrine constraining government intrusion on communications generally could be based on Justice Brandeis’ dissent in \textit{Olmstead v. U.S.}. Recognizing that the protections enumerated in the Constitutional Amendments must be given broad scope, Brandeis
stated:

The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man’s spiritual nature, of his feelings and his intellect…

They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men. To protect, that right, every unjustifiable intrusion by the government upon the privacy of the individual, what ever the means employed, must be deemed a violation of the Fourth Amendment.

Thus courts could protect communications from governmental intrusion by broadly interpreting the Fourth Amendment to give a general protection from unauthorized governmental intrusions. Such protections could be extended to new technologies as they are developed.

In *Katz v. U.S.*, the Supreme Court adopted much of Brandeis’ reasoning. The *Katz* Court stated that whatever a person “knowingly exposes to the public even in his own home or office, is not subject to Fourth Amendment Protection … [but what a person] seeks to preserve as private, even in an area accessible to the public, may be Constitutionally protected.” However, the Court declined to expand the protections beyond the scope of government intrusions on privacy that were not authorized by a magistrate. The government is therefore constrained from intrusions that are not authorized by a judicial actor. Thus there already exists a foundation for courts to protect the privacy of communications, where there is a reasonable expectation of privacy, without regard to the medium from government intrusion.

Because the *Katz* Court refused to extend a general right to be left alone, communications must be given additional protections from nongovernmental parties. In fact, such a tort was proposed in Brandeis and Warren’s *The Right to Privacy*. Courts have already found liability for wiretapping under the “unreasonable intrusion” rubric of invasion of privacy. It would be only a small step to add Internet-based communications to the protected class of communications, and thereby provide a remedy against civilian actors.

Therefore, by implementing this framework, the courts could protect communications that have been adopted by the public but are not yet covered by the wiretapping laws. Using the reasoning employed in *Katz*, courts could protect new communications from interference by governmental actors. Communications could be similarly protected from civilian interception by expanding the tort of invasion of privacy. Furthermore, as the protection of the framework is based upon individual rights rather than particular technologies, the framework will protect communications without regard to the mode of transmission. Thus, the framework will protect the Internet-based communications at issue in the recent wiretapping cases, as well as communications over technologies which have not yet been invented.

“Technology-independent laws would not seek to replace laws that regulate the issues specific to a given technology, but rather they would work hand in hand with the more specific law.”
2. The implementation of such a framework could prove to be significant undertaking.

However, this framework is unlikely to be uniformly adopted. The solution necessarily involves many different actors. Each court would create its law based on the cases that come before it, leaving open the possibility that widely disparate opinions would be handed down. The variance in state invasion of privacy torts could lead to complicated jurisdictional fights. Further, Internet-based communications allow a user in one state to retrieve information from servers in other states. Thus, a court wishing to find liability for invasion of privacy for intrusion into Internet-based communications would first have to find the correct law to apply. Conceivably, the court could be faced with the choice of the law of the plaintiff’s state, the law of the state where the server is located (arguably the location of the breach), and the law of the defendant’s state. Each state’s law could prove beneficial to a different party, and, as such, would surely lead to bitter choice of law disputes. These complications would make the invasion of privacy route difficult at best.

Furthermore, creating such a framework would require a certain level of judicial activism with which many judges would be uncomfortable. By applying this framework to new technologies the courts would arguably be creating new law, an unattractive prospect for many judges.

D. The Broad Legislative Solution: Technology-Independent Laws

The best solution would entail Congress creating laws which protect communications in the abstract without dealing with technological specifics. Such laws would avoid the uniformity problems of the judicial framework because they would be adopted on a federal level. These technology-independent laws would lay out in abstract terms the protections that are offered to communications. Technology-independent laws would not seek to replace laws that regulate the issues specific to a given technology; rather, they work hand in hand with the more specific law. The more specific, technology-dependent laws would relate to the technology-independent laws much as administrative regulations relate to congressional legislation. That is to say that they would create solutions to the specific problems that the technology raised. Technology-independent laws would essentially be statements of principles that judges could use to decide cases involving new technology until laws pertaining to the specific technology have been created. Judges would be given the guidance they need to rule on issues pertaining to a specific technology even though the legislative bodies have not yet addressed it. As the laws would not address specific technologies, they would not become obsolete when new technologies are created.

Further, as the technology-independent laws would not be constrained by innovations, they would address problems such as those raised in the recent circuit court cases. The courts will be able to decide these cases even though the technology does not fit within the four corners of the wiretapping laws because Congress will have given them broad guidance with which to do so. Thus, a broad legislative solution would solve the immediate problem created by Internet-based communications, as well as the broader problem of legal obsolescence.

1. The underlying principles of the broad legislative solution

While any legislative solution as broad as the one proposed would be the subject of much debate and compromise, one can speculate about the broad contours of such a solution based upon the current laws. A common requirement is that protected communications must be reasonably believed to be private. Thus a broad statutory protection should begin with the statement that all communications reasonably believed private are to be protected from unwanted intrusions of any kind.

Furthermore, the courts and Congress have not left the right to privacy in communications unfettered. For example, the law allows for government intrusion when a magistrate deems such intrusion necessary to prosecute criminal activity. Moreover, private interventions by service providers are allowed when they are necessary to maintain the service.
any abstracted law must allow for reasonable interventions by government and service providers. The extent of the interventions would be a matter for debate.

2. An example of a law based on the above principles

Based on the preceding considerations, and borrowing heavily from the present wiretapping laws,186 the following act could be proposed:

§ 1. Definitions

As used in this title –

1) “protected communication” means any form of human interaction, be it oral, aural, visual, electronic, or otherwise, conveyed by a person exhibiting an expectation that such communication is not subject to interception under circumstances and not intended for public dissemination;

2) “intercept” means the acquisition of the contents of a protected communication by any unauthorized party;

3) “unauthorized party” means any person not intended to receive or comprehend the contents of a protected communication;

4) “contents” means any part of a human interaction;

5) “person” means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, corporation, or other legal entity.

§ 2. Interception of Protected Communication

(1) Offense. – Except as provided in subsection (2) of this section, an unauthorized party who –

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any protected communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any protected communication;

(c) intentionally discloses, endeavors to disclose, or procures any other person to disclose or endeavor to disclose any protected communication;

(d) intentionally uses, or endeavors to use, the contents of any protected communication, knowing or having reason to know that the information was obtained through the interception of a protected communication in violation of this subsection;

shall be punished as provided in subsection (3) or shall be subject to suit.

(2) It shall not be unlawful for —

(a) a law enforcement official, duly authorized by a magistrate and during the course of official duties;

(b) a person or entity of providing communication service whose assistance has been request by a person described in part (a) of this subsection or who is performing functions deemed essential to the maintenance and assurance of the quality of their service;

to intercept protected communication.

(3) whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

3) The broad legislative solution would solve both the narrow and broad problems posed by the recent decisions

Creating a more abstract law protecting the privacy of communications would add a measure of certainty to the interactions of law
and new technology. It would not prevent the creation of more specific laws that fit within the overall framework, rather it would merely give judges guiding principles to aid in their decision-making. By creating a statutory framework, Congress will provide the courts with the tools to deal with technologies that do not fit within more specific laws and ensure that the law applies uniformly across diverse jurisdictions.

IV. Conclusion

Our present information age is marked by rapid changes in technology. People have become increasingly willing to adopt new innovations in their daily lives. While it is possible that some dystopic horror such as those illustrated in early Mel Gibson films could occur, this scenario is highly unlikely. Thus, we must assume that society will continue to make technological improvements at or above its present rate.

The changing technology will necessarily make technologically-based law obsolete. The evolution of the wiretapping laws shows that when laws are designed around a specific technology, they will be vulnerable to obsolescence due to technological changes. The wiretapping laws were first created to address the needs of a communications network based around a large monopoly, and they necessarily needed revision when that monopoly was broken up. More recently, the present laws have been held to not apply to new Internet-based forms of communications.

When laws become obsolete because their underlying technology has passed out of popular use, society suffers. During the time between the obsolescence of the law and the creation of new law applicable to the new technology, there is uncertainty leading to lowered rates of technology adoption and the attendant efficiency gains. Thus, the law must find a way to address areas of rapid technological change.

The creation of technology-independent laws will reduce uncertainty by giving judges guiding principles by which to address new technologies. These laws would not seek to replace laws specifically tailored to the needs of particular technologies. Rather, they would more abstractly state the underlying principles of the law relating the area of a particular technology and thereby apply to all technology in the area whether old or new. By creating technology-independent laws, the legislators may ensure that there will be continuity in the law even if the technologies which the law addresses are in flux.

ENDNOTES

1 Ben Schott, Schott’s Original Miscellany 148 (First U.S. Ed. 2003).
3 Id.
6 See The Matrix (Warner Studios 1999); The Terminator (Orion Pictures 1984); Blade Runner (Warner Studios 1982).
9 See infra Part II.D.
See infra Part III.A.

See infra Part IV.D.

Ex Parte Jackson, 96 U.S. 727, 733 (1877).

Id.

Id.


See infra Part II.C.


See infra Part II.C.2.

See infra Part II.B.


Id. at 194.

Id.

Id.

Id. at 195–96.

Id. at 200–05.

Id.

Id.

Id. at 215–18.

Other foundations for the tort include: libel law, the Fourth Amendment, trespass, criminal eavesdropping laws, and injunctions preventing publication of private letters. Bratman, supra note 20, at 633–34.

See infra Part II.C.1.


Id. The tort is usually divided into four varieties: appropriation (using a person’s name or likeness without permission), unreasonable intrusion (intentional interference into a person’s body or affairs), public disclosure of private facts, and false light in the public eye (publication of sensitive personal matters). Id.


Prosser & Keeton, supra note 32, at 851. Rhode Island is the only jurisdiction which does not recognize invasion of privacy. See id.

Id. at 854.

Id. at 855.

Id.

Id.

Id. at 854-55.


See infra Part II.C.2.

See infra Part II.C.2.

See infra Part II.C.3.
48 Id.
49 Id.
50 Id. at 464.
51 Id.
52 Id. at 466.
53 See id. at 471 (Brandeis, J., dissenting).
54 See id. at 475.
55 Id.
56 Id. at 474.
57 Id. at 478.
58 Id. at 469.
60 Id.

61 Katz, 389 U.S. at 348. In Olmstead, the Court held that the Fourth Amendment was designed to protect from physical seizures, and thus the Amendment’s application is limited the realm of tangible, physical objects. Olmstead v. United States, 277 U.S. 438, 474 (1928).
62 Katz, 389 U.S. at 349.
63 Id. at 351.
64 Id. at 359.
65 Id. at 353.
66 Id. at 351.
67 Id. at 358.
68 Id. at 350–51.
69 Id.

70 See supra Part II.B.
73 Id.
74 Id. That is, communications that could be overheard by the human ear and that were made over the monopolistic telephone carrier.
75 Id.
76 Id.
77 Id. at 5.
78 Id. at 2.
79 Id. at 1.
80 18 U.S.C. 2517 (2004) (Congress substituted “wire, oral, or electric communications” in place of “wire or oral communications.”).
81 Id.
82 Id.
83 Id.
84 Id. § 2511.
85 Id.
86 Id. § 2510(4).
87 Id. § 2510(2).
88 See id.
89 Id. § 2701.
90 Id. § 2701(a)(1).
91 Id.
92 Id. § 2701(c)(1).

Steven Jackson Games, Inc., 36 F.3d at 459.

Id.

Id.

Id. at 461 (stating that “the definition of ‘electronic communication’ does not include electronic storage of such communications”).

Id.

302 F.3d 868, 878 (9th Cir. 2002).

Id. at 872.

Id. at 873.

Id. at 878.

155 F.3d 1051, 1058 (9th Cir. 1998).

Konop, 302 F.2d at 878.

Id.

United States v. Steiger, 318 F.3d 1039, 1048 (11th Cir. 2003) (holding that evidence obtained by an anonymous hacker through use of a Trojan Horse should not be suppressed as violating the Wiretap Act); Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3rd Cir. 2004) (holding that an insurance company did not intercept its agent’s e-mail when it accessed his e-mail on the central file server and that the company’s actions were protected under the SCA’s service provider exception).

See supra Part II.D.


See infra Part III.A.

See infra Part III.B.

See Jessica Steinberg, The VoIP revolution takes hold, JERUSALEM POST, Dec. 10, 2004, at Economics 15 (“Voice over IP allows the transmission of voice, video and data over Internet networks.”).

Id.
Protecting the Future


129 Id.

130 Id.

131 Id.

132 Id.

133 Id.

134 Id.

135 See supra Part II.D.

136 Id.

137 Id.

138 See supra note 121.

139 Fred O. Williams, Phone Service Over Internet Causes Static for Some Users, BUFFALO NEWS, Dec. 19, 2004, at C1.

140 Tom McGhee, VoIP might be telecoms’ link to revival, DENVER POST, Jan. 2, 2005, at K1. This communication method has been gaining in popularity; the Ford motor company recently switched to a similar system. Paul Travis, Ford Trades Up to IP Telephony System, INFORMATION WEEK, Sept. 27, 2004, at 22.

141 Andrew Backover, How Do Internet Phone Calls Work?, USA TODAY, Dec. 12, 2003, at 7B.

142 Peter J. Howe, Wiretap Law To Apply to Net Calls, BOSTON GLOBE, Aug. 5, 2004, at C2.

143 See supra Part II.D.

144 See SCHUMPTER, supra note 2.


146 Id.

147 Id.

148 See, e.g., Steven Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 459 (5th Cir. 1994).

149 Id.

150 See supra Part II.D.

151 See, e.g., Fraser v. Nationwide Mutual Insurance Company, 352 F.3d 107, 114–15 (3rd Cir. 2004) (opining that “[w]hile Congress’s definition of “intercept” does not appear to fit with its intent to extend protection to electronic communications, it is for Congress to cover the bases untouched.”).

152 For example, a phone call placed on a traditional landline would be protected from unauthorized wiretapping under 18 U.S.C. § 2511. A phone call placed over a VoIP system does not appear to receive the same protection. See supra Part III.A.

153 For a fuller discussion of the economic effects of uncertainty, see THOMAS SOWELL, BASIC ECONOMICS: A CITIZEN’S GUIDE TO THE ECONOMY 191–242 (revised and expanded ed. 2004).

154 Id.

155 Id.

156 373 F.3d 197, 204 (1st Cir. 2004) (Lidez, J., dissenting).

157 Id. at 211.

158 Id. at 212.

159 Id. at 210–11.

160 Id. at 219.

161 Id. at 216.

162 See supra Part II.D.

163 See supra text accompanying note 152.

164 See supra Part II.D.
Nation in Brief, WASH. POST, Oct. 21, 2004, at A13 (stating “the 9th Circuit in San Francisco, widely considered one of the most liberal and activist in the country…”).

Charles Lane, Court Hears Argument on Race Bias in Capital Case, WASH. POST, Dec. 7, 2004, at A3 (stating “the 5th Circuit, which covers Texas, Louisiana and Mississippi and is considered one of the more conservative federal appeals courts”).

Steven Jackson Games Inc. v. United States Secret Service, 36 F.3d 457, 459 (5th Cir. 1994); Konop v. Hawaiian Airlines, Inc. 302 F. 3d 868, 878 (9th Cir. 2002).


Id.


Id. at 351.

Id. at 350, 356.

Id. at 350.

Warren & Brandeis, supra note 21, at 193.

See supra Part II.B.

Katz, 389 U.S. at 350.

See supra Part II.D.

See supra Part IV.C.

See supra Parts II.D. and III.A.

See, e.g., Katz, 389 U.S. at 351–53.