1-1-2011

The Fourth Amendment and Cyberspace: Conflict or Cohesion?

Federico Alberto Cantón
Portland State University

The Fourth Amendment and Cyberspace: Conflict or Cohesion?

by

Federico Alberto Cantón

A thesis submitted in partial fulfillment of the
requirements for the degree of

Master of Arts
in
Political Science

Thesis Committee:
Chris Shortell, Chair
Craig Carr
David Kinsella

Portland State University

Abstract

The purpose of the study was to determine how the Fourth Amendment is treated in the age of the internet. To determine the degree of the significance of this relationship a comparative approach is used. Court opinions from cases involving other technological innovations and the Fourth Amendment were examined and their reasoning was compared to that of cases involving the internet and the Fourth Amendment. The results indicated that contrary to some fears that the internet would require a different approach with respect to the law it actually did not present many novel barriers to its application. The principle conclusion was that the reasoning used in cases involving older technologies, namely the test outlined in *Katz v. United States*, was consistently applied even in the age of the internet.

Table of Contents

Chapter 1: Introduction and Literature Review

The invention and subsequent proliferation of the internet has impacted not just our society but others around the world. With such a large sphere of influence it could therefore be expected that there are instances in which people's actions in cyberspace may come in conflict with the law. This type of conflict will be at issue in this work, yet it will be more narrowly approached. The question posed here relates to the relationship between the law and the internet. There are many potential approaches possible when one tries to examine this relationship. The one used here focuses on the manner in which U. S. courts treat Fourth Amendment issues on the internet. The relationship between the law and the internet is important to a degree extending beyond merely the Fourth Amendment because ultimately laws that concern the internet can alter the way in which individuals behave on it.

The internet is an arena where people partake in countless actions varying from personal to business-related. Therefore a law that is crafted in order to govern what may or may not be performed on the internet could have significant implications for many people. One extreme example may be that if a law were passed that made it legal for police to read a suspect's e-mails without a warrant, then such a law is likely to curb the amount of e-mailing many people do. The manner in which the law and the internet interact is therefore far from trivial when one realizes it could potentially shape people's behavior.

Given that the internet is such a large technological innovation the question may be raised whether courts can treat Fourth Amendment cases exactly as they do their real-world counterparts, whether they adapt their interpretations of laws accordingly, or if

they interpret the relationship in a wholly new manner. From the findings obtained when examining this subset of the law a clearer understanding of the larger relationship between the law and the internet could then be formed. Lessig more generally approaches this question, asking "should this new space, cyberspace, be regulated by analogy to the regulation of other space, not quite cyber, or should we give up analogy and start anew" (1995, 1743)? Furthermore Lessig questions whether there is anything truly new about cyberspace; "is there really a form of life here that we haven't known before, or is cyberspace just an electronic version of ordinary space, where the electronics might add something, but not really very much (1995, 1743)? Examining how Fourth Amendment cases are treated on the internet could then help in more concretely answering these questions.

The basis for the inquiry outlined above is grounded in past technological advances and the manner in which the courts have responded to Fourth Amendment issues related to them. Aerial surveillance, beepers, wire taps, and thermal imagers are examples of technological advancements that have had run-ins with the Fourth Amendment. The common law system under which the U. S. operates as well as the principle of *stare decisis* would imply that past cases concerning the same subject are expected to be resolved similarly, or at least using similar reasoning. These two principles combined with the observation that Fourth Amendment cases have been decided based on the same principles even when they concerned different technological innovations would further strengthen the path taken here. To support the observation noted above it should be mentioned that, taken as a whole, the manner in which courts have interpreted the Fourth Amendment vis-à-vis these technologies has been grounded

in the same fundamental principles, these being those derived from Justice Harlan's concurring opinion in *Katz v. United States*. Justice Harlan's concurring opinion in *Katz* has become the standard by which unreasonable searches and seizures are judged. This "reasonable expectation of privacy" test was later more clearly stated in *Smith v. Maryland* as a test with two steps:

> The first is whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy,' whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve [something] as private.' The second question is whether the individual's subjective expectation of privacy is 'one that society is prepared to recognize as `reasonable,'' whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances. (*Smith v. U.S.*, 1979)

Both *Katz* and *Smith* dealt with Fourth Amendment issues raised due to technological advances. *Katz* dealt with an electronic eavesdropping device and *Smith* dealt with a pen register, which is a device that records the numbers that are called from a phone line. Other cases that followed the test outlined in *Katz* and involved other forms of technology are *United States v. Karo* and *United States v. Knotts*, both of which dealt with monitoring an individual via an electronic beeper. Given that Fourth Amendment questions about these past technological innovations were addressed by looking to the same fundamental principles, if cases concerning the internet are interpreted differently by the courts then this could indicate that cyberspace is a truly unique environment in need of a wholly new approach with respect to the law, although this may be an extreme

scenario. On the other hand to find that the Fourth Amendment questions examined her are treated much as they were before this would at the very least show that some portions of real-world law may be more easily applicable to the cyber-world.

To further emphasize the potential import of the question posed here it would perhaps help to frame the issue within the context of the schools of thought that see cyberspace as being amenable to the law on the one hand and those that do not feel that the law can be applied so easily to the internet on the other. Goldsmith (1998), for example, is one of the scholars that focus on the question of whether or not cyberspace is able to be regulated at all. He points out that there are many skeptics doubting the possibility of there being a positive relationship between the law and cyberspace, noting that such skeptics may claim that "cyberspace is so different from other communication media that it will, or should, resist all governmental regulation" (1998, 1201). To find that the relationship between cyberspace and the Fourth Amendment is comparable to other past technological innovations would then not only complement Goldsmith's claim that "regulation of cyberspace is feasible and legitimate from the perspective of jurisdiction and choice of law" but it may also undermine to a degree some of the skeptic's notions of cyberspace (1998, 1201).

Lawrence Lessig also speaks to the issue of the viability of there being laws in cyberspace. Lessig (1999) disagrees with the skeptics that question whether the internet is amenable to regulation at all. His approach to the issue is a structural one, noting that some skeptics' opinions of cyberspace are that "the nature of the space makes behavior there *unregulable*" (Lessig 1999, 505). He disagrees, however, because such a view relies

on the assumption that cyberspace cannot adapt. Instead Lessig claims about cyberspace that:

> Its architecture is a function of its design -- or … its code. This code can change, either because it evolves in a different way, or because government or business pushes it to evolve in a particular way. And while particular versions of cyberspace do resist effective regulation, it does not follow that every version of cyberspace does so as well. Or alternatively, there are versions of cyberspace where behavior can be regulated, and the government can take steps to increase this regulability. (1999, 506)

Once again delving into the relationship between the Fourth Amendment and the internet may shed light into how the law functions within this structure of cyberspace. To find that Fourth Amendment cases online are treated much like other Fourth Amendment cases fits into this more general debate between those in favor and those opposed to regulation given that it shows that the gap between the real-world and the cyber-world can indeed be bridged. From a strict adherence to past reasoning, to starting anew, or some middle ground, the manner in which courts treat these cases could shape, or be shaped by, the development of this relationship. In this sense the manner in which the courts treat the relationship between the Fourth Amendment and the internet could impact what "version of cyberspace," as Lessig puts it, is in effect. Such an inquiry is beyond the scope discussed here but could be a potential area of further research.

As mentioned, however, there are also those that do not so readily accept the possibility that the internet is as easy to regulate as some may think. Johnson and Post (1996), for example, base the crux of their argument against regulation of the internet on

the notion of territorial borders. Johnson and Post appeal to the connections between the real-world and the cyber-world to support their claims. They use the differences between the two worlds as being the reason why the law is not as readily amenable to cyberspace. It is fairly obvious that in the real world "territorial borders, generally speaking, delineate areas within which different sets of legal rules apply" (Johnson and Post 1996, 1367). The problem with applying real-world laws to the internet should then be readily evident, namely "cyberspace has no territorially based boundaries, because the cost and speed of message transmission on the Net is almost entirely independent of physical location" (Johnson and Post 1996, 1370). For Johnson and Post the attempts by governments to then try to regulate actions on the internet is a futile endeavor to undertake given that "the volume of electronic communications crossing territorial boundaries is just too great in relation to the resources available to government authorities" (1996, 1372). Furthermore they claim that even an attempt to create borders in cyberspace may be nearly impossible "because the Net is engineered to work on the basis of 'logical,' not geographical, locations, any attempt to defeat the independence of messages from physical locations would be as futile as an effort to tie an atom and a bit together" (Johnson and Post 1996, 1374). This type of argument is precisely the kind that Lessig (1999) addressed when he argued against the skeptics.

While Johnson and Post do not believe that real-world laws can be readily transplanted to cyberspace they still recognize that there is a necessity for a system to address legal issues arising in cyberspace. Their solution to the problem, however, is based on "conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'" (1996,

1378). Under this conceptualization by considering cyberspace as a homogenous space within the law then the problems raised by real-world borders fall by the wayside.

Bomse (2001) also notes that the structure of the internet is perhaps the prime argument made by those that oppose regulations but beyond this there are other reasons. Another argument that is made against internet regulation is based on the perception that government is "antithetical to the rapidly changing, highly versatile character of the computer industry" (Bomse 2001, 1727). Furthermore, even if government has the best of intentions with respect to regulating the internet, it functions much too slowly when compared to the rate at which the internet evolves (Bomse 2001, 1728). If these claims are true then any laws applied to the internet by the government may indeed be detrimental given that they would be outdated by the time they went into force. These alternate claims made against regulation that Bomse states could also be addressed by examining the way in which courts treat Fourth Amendment issues on the internet. The ease with which courts arrive at their rulings as well as the rulings themselves could indicate the responsiveness of the government to the quickly changing world of cyberspace.

There are others that are not as skeptical when it comes to the possibility of applying the law to the internet, instead they emphasize what may be important is the approach taken when attempting to do so. This does not mean, however, that they may feel old laws are directly applicable to the internet. Kerr acknowledges that there are scholars that "believe that the field of Internet law offers nothing new," to them "applying law to the Internet is like applying law to any new set of facts: draw analogies and then apply existing law" (2003, 380). For Kerr the statements made by those skeptics

of internet law, or “cyberlaw” as he calls it, are not as easily applied as they may think given that the proper analogies would depend on the particular perspective that is adopted. Neither does he wholly agree with those that support the idea of cyberlaw given that he does not think a complete change is needed when approaching law in cyberspace, it is mainly the way in which the facts are approached that needs to be addressed.

Kerr frames the problems related to applying the law to the internet as stemming from determining what the “facts” are. He views the answer to this problem as taking one of two forms:

> We can model the Internet's facts based on virtual reality, looking from the perspective of an Internet user who perceives the virtual world of cyberspace and analogizes Internet transactions to their equivalent in the physical world. Alternatively, we can model the facts based on the physical reality of how the network operates. From this perspective, Internet transactions can be understood based on how the network actually works "behind the scenes," regardless of the perceptions of a user. (Kerr 2003, 357)

To be able to apply the law to the internet it must be determined which of these perspectives to adopt. Kerr labels the perspective that bases facts on virtual reality the “internal perspective,” and the perspective based on real-world facts the “external perspective.” The perspective chosen is important, Kerr claims, because it can influence how law shapes out on the internet given that “in a surprising number of situations, we arrive at one result when applying law from and internal perspective and a different result when applying law from an external perspective” (2003, 357). The reason behind these

varying outcomes according to Kerr is that each perspective is bundled with its own set of facts and "legal outcomes depend on facts, and the facts of the Internet depend on which perspective we choose" (2003, 361). Furthermore Kerr argues that each set of facts do not necessarily have to correlate. Changes one may experience in one realm are not necessarily reflected in the other. A change in code may drastically impact a person's online experience but a physical change, for instance relating to wiring by an ISP, may go completely unnoticed by the user. Therefore, given that the two sets of facts need not coincide "every time we apply law to the internet, we will have two possible outcomes: an internal outcome and an external outcome" (Kerr 2003, 362).

Kerr illustrates the potential impact these different perspectives may have by presenting the approaches two officers may take with respect to email. He argues that one officer, viewing email from the internal perspective, will see an email sent from one person to another as a virtual manifestation of physical mail. This officer would conclude that to access email would require a warrant according to the Fourth Amendment. A second officer, looking at the situation externally, would arrive at a different conclusion. The second officer would merely view the transmission of the email as a message relayed first to the user's ISP who copies the message and then sends it to the recipients' ISP, if they do not share the same ISP, who would then in turn send the recipient a copy of the message when the recipient requests it by clicking an icon on their computer. This officer would view the email as a message that has been transmitted to several parties, requiring only a subpoena to retrieve it from one of the intermediaries and not a search warrant (Kerr 2003, 365-366).

Ultimately Kerr does not venture a guess as to which perspective should dominate, claiming that "perhaps one of these influences will overpower the other, establishing a more internal or external approach over time" or alternately "perhaps an equilibrium will be reached, and both perspectives will survive and continue to shape the law of the Internet in the future" (2003, 405). His view stands in between the extremes consisting of those who claim that the law cannot be applied to the internet on one end and those that argue it can be applied without any special attention on the other. For Kerr the old laws can be applied, but there may be some form of adaptation that needs to take place in order for this to occur.

In a later article Kerr notes the persistence of the problem of adapting old laws to the internet and focuses more closely on the Fourth Amendment. Kerr notes that "a few scholars have pointed out that the application of the Fourth Amendment to computer networks will require considerable rethinking of preexisting law, but none have sketched out what that rethinking might be" (2010, 1006-1007). He also reiterates that "the differences between the facts of physical space and the facts of the Internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment" (Kerr 2010, 1007). Both of these claims highlight how Kerr does feel that while previous laws can be applied to the internet, they must first undergo some changes. Though one may at first think this would require fundamental changes to how courts treat Fourth Amendment issues online, Kerr recommends that "courts should try to apply the Fourth Amendment in the new environment in ways that roughly replicate the role of the Fourth Amendment in the traditional physical setting" (2010, 1007). This view then does not go so far as the one

calling for a complete reconceptualization of how the law is meant to function with respect to the internet.

Kerr argues for some smaller scale adaptation of the law, however. He claims that such a new approach is needed given that "as technology advances, legal rules designed for one state of technology begin to take on unintended consequences" and "if technological change results in an entirely new technological environment, the old rules no longer serve the same function" (Kerr 2010, 1009). The new rules in turn are not meant to create more change, however, they are rather meant to allow the older rules to function once again in the new environment. Kerr's overall view of the Fourth Amendment with respect to the internet is that it "will have to adopt new principles to maintain its longstanding function" but "the need for evolution is nothing new: the Fourth Amendment will adapt to how wrongdoers use the Internet just as it adapted to how wrongdoers started using postal letters, automobiles, and the telephone" (2010, 1048). What is important for Kerr is to develop a way to be able to bridge the old laws to the new environment.

By clearly identifying adequate links between the real world and the cyber world Kerr argues that "the Fourth Amendment will remain technology-neutral in the sense that the overall amount and function of Fourth Amendment protection will be roughly the same regardless of whether a wrongdoer commits his crime entirely online, entirely in the physical world, or using a mix of the two" (2010, 1015-1016). Through recognizing that the two environments are distinct but then trying to create adequate links between them Kerr believes that the more fundamental goals of the Fourth Amendment will adapt in the face of new technologies.

As in his previous work Kerr emphasizes how facts are important when it comes to the relationship between the Fourth Amendment and the internet but this time around he goes further and argues how facts can help to bridge the gap between these two. He focuses on the inside/outside distinction in the physical world, claiming that it serves to "distinguish between what the police can do without cause and what they need cause to do" (Kerr 2010, 1009). Yet noting that there is no inside/outside that is readily identifiable online Kerr asks "what rule or standard in the online setting can server the same basic function that is served by the inside/outside distinction in the physical world" (2010, 1018)? The answer to this question according to Kerr is to relate inside/outside surveillance to content/non-content surveillance online. The reason given for this is that when police watch someone outside they can gather information such as where they were, what they were doing, or where they were going at a particular time. Inside surveillance would consist of breaking into a person's private space which would lead to the gathering of more personal and private information. Similarly, Kerr suggests that "online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private thought and speech" (2010, 1018). By examining the reasoning that courts use with respect to Fourth Amendment cases involving the internet it could potentially be observed whether courts have put the kind of comparisons Kerr points out between the real and online worlds in effect, which would in turn be indicative of some degree of adaptation of the Fourth Amendment in the face of the internet.

Kerr is not alone in arguing that a distinction must be made between the physical and digital worlds when applying older laws to the internet. Tyson (2010) also argues that

"courts should more closely scrutinize the distinction between the content and non-content portions of an internet communication rather than rely on antiquated doctrines that do not adequately address all of the possible privacy concerns" (2010, 1261). Tyson's approach to the problems arising from the interaction between the internet and the Fourth Amendment revolves around statutory attempts taken to address them. The statute that Tyson focuses on is the Stored Communications Act. Tyson acknowledges that even a statutory approach may have its shortcomings, claiming that "the SCA fails to adequately protect an Internet user's privacy because it lacks suitable guidance for the courts to follow when interpreting the statute" (2010, 1284). An example of this failing is that "the SCA distinguishes between content and non-content in an Internet communication, but it does not provide the courts with clear guidance to determine the difference between content and non-content in light of changing technology" (Tyson 2010, 1284). Furthermore while some have argued that courts work too slowly to keep up with technology Tyson suggests that statutes may also not adapt as quickly as one may expect, claiming that "Congress has not updated the SCA quickly enough to reflect modern Internet use, and thus, the SCA has failed to keep pace with the rapid development of Internet communications" (2010, 1285). Ultimately Tyson favors a judicial rather than statutory approach in order to better address the friction that may arise between the Fourth Amendment and the internet, mainly because "the SCA does not provide a suitable substitute for Fourth Amendment protections because modern Internet use has outgrown the SCA's useful application" (2010, 1298). Yet she argues that courts cannot merely proceed as they have if the best outcome is to be attained, rather "courts should recognize that the first generation of Internet privacy decisions relied on

antiquated doctrines and that these decisions might not help a modern court resolve privacy questions" (2010, 1298).

Grubins (2008), similarly to Tyson and Kerr, believes there is potential for the law to be applied to the internet but in order to best do so it must be adapted in some manner. Furthermore, similarly to Tyson, Grubins questions which approach may be best for dealing with the issues that may arise when the internet comes into conflict with the Fourth Amendment; legislative, judicial, or a mix of the two? Of the statutory attempts made to protect privacy Grubins claims that what they actually protect is rather narrowly defined and that "these limited provisions do not address the broad, ongoing changes in communications technologies" (2008, 741). Grubins also points to Voice over Internet Protocol (VoIP) technology to demonstrate how statutes may be detrimental to privacy. While a VoIP call is overall very similar to a regular phone call Grubins argues that given the way it functions mechanically it may fall under the purview of either the Stored Communication Act or the Wiretap Act, which would offer different degrees of protection. This type of argument could be seen as another example to the idea Kerr (2003) posited regarding internal and external perspectives, demonstrating how both courts and Congress may grapple with similar issues when trying to apply the law to the internet. Grubins then weights the benefits and consequences these two bodies hold when it comes to dealing with the issue of the law on the internet.

Grubins notes that "the fast pace of technological development might appear to favor legislative leadership" given that "in theory, legislatures are able to respond quickly to changes in technology by updating legislation regularly" (2008, 744). Yet, similarly to Tyson, Grubins claims that even though Congress may appear to have the capacity to

deal with these issues it "does not always amend the statutory framework to keep up with changes in technology, which can lead to outdates laws and insufficient protection" (2010,744). Another claim often made to support the statutory approach to dealing with internet and privacy issues is that Congress has the benefit of holding committee meetings wherein they can be better informed by experts to potentially choose the best path to take when deciding the issues, yet Grubins counters that this means that Congress "is subject to political realities that do not always make it the best arbiter of constitutional provisions; it may not be able to give equal weight and consideration to all interests" (2010, 745). Similarly along this line of reasoning is the claim that "Congress is also easily swayed by public opinion" meaning that "such a system responds well to the wishes of the majority, but public fear and outcry can lead to laws that do not give sufficient weight to constitutional concerns or protect all interests" (Grubins 2010, 746). While there are also those that argue against an overly active court Grubins claims that Fourth Amendment jurisprudence "supports a judicial system that actively reinterprets and applies Fourth Amendment privacy protection as new technologies develop" (2010, 748). Furthermore Grubins notes that an added benefit to the judicial approach when compared to the legislative one is that "legislatures act without regard to constitutional requirements and the freedom from government intrusion, so highly valued by the Constitution's framers, can be easily eroded" (2010, 748). Ultimately Grubins' favored approach is for a combination of both approaches. Courts can lay the baseline privacy expectations that may come along with technological innovations, but "no court decision would be able to address all factual scenarios, so congressional refinements would be

necessary" (2010, 751). The congressional refinements would be added with the knowledge that courts place a strong premium on the privacy in the new technologies.

Leary (2011) questions the applicability of the Fourth Amendment to new technologies as well. Though her approach is narrowly focused, in that it questions how the Fourth Amendment and technology impact society's youth, she raises a larger issue that may be made about the expectation of privacy present in this day and age. Leary points to the test established in Katz in order to demonstrate how it could potentially create problems with respect to today's youth. The reason behind this problem derives from the notion that youth and other "digital natives" often "engage in somewhat risky behavior online and have a false perception of privacy" (Leary 2011, 1071). As a result of this naïveté these individuals "may not manifest a subjective expectation of privacy similar to adults" (Leary 2011, 1071). In this sense then the Katz test would be potentially unfairly applied to an entire class of society. Leary's fundamental question is that "given that many youths arguably seem to act differently about traditionally privacy online, how can the law plausibly rule that they nevertheless have a reasonable expectation of it" (2011, 1072)? The problem stems from the tendency of youths to all too readily through conditioning share their private information online; to them it is the natural order (Leary 2011, 1089-1090). So if a young person was somehow able to establish a subjective expectation of privacy, with respect to the objective prong of the Katz test the question of who is used as the norm becomes important, what may seem reasonable to the youth would perhaps be not as reasonable to the rest of society who may be more reticent to reveal information as freely online. When viewed from the perspective of the debate between the ability or lack thereof to apply the law to the

internet Leary's work would fall somewhere in between the two extremes. On the one hand she does not completely doubt that the law, in this case the Fourth Amendment specifically, can be applied online. Yet she warns that it can potentially be applied unfairly and may therefore need to be adapted in order to remedy this problem.

The difficulty outlined by Leary (2011) with applying the Fourth Amendment to new technologies is expanded upon by Plourde-Cole (2010). Plourde-Cole points out that with respect to the Katz test "the second prong's supposedly objectively inquiry – the question of whether society 'recognizes' as reasonable a certain privacy right - is one that is objectively unanswerable by judges, philosophers, or even sociologists" (2010, 580-581). Plourde-Cole goes beyond arguing that the Katz test may not be readily applicable to the youth, as Leary does, and questions whether it can be accurately applied at all. Furthermore she notes that "the challenge of discerning an 'objective' standard for whether a privacy expectation is reasonable is exacerbated by the rapid evolution of technology, where expectations are neither static nor easily discernable" (Plourde-Cole 2010, 581). In this sense it appears as if Plourde-Cole favors the adoption of wholly new principles in order to best apply the law to the internet, at least to the degree that the Fourth Amendment is concerned.

Orso (2010) and Engel (2010) both build upon the extant difficulties in the relationship between the internet and the law, emphasizing the import of addressing these issues. Both of these scholars' works take the problems presented between the internet and the Fourth Amendment and go beyond merely examining the internet on computers to include the problems posed by the internet on smartphones. The internet and cellular phones are still relatively new innovations whose relationships with respect to the law are

still far from fully defined. As the previously mentioned authors have made clear the relationship between the internet and the law can be troublesome. Smartphones further complicate this situation given that they combine these two innovations and bring about even more questions that need to be addressed.

With respect to computers Orso notes that "there is a dearth of search incident to arrest jurisprudence regarding laptops or personal computers" (2010, 224). This lack of a reference point complicates the situation with smartphones since although they are phones as their name implies they can perform many of the same functions that a computer can. Therefore one may question if these phones may instead be evaluated according to jurisprudence related to phones. Orso notes that contrary to what one may assume with respect to cellular phones "federal courts have validated warrantless searches of cellular phones, usually relying on one of two exceptions to the warrant requirement – exigent circumstances and search incident to arrest" (2010, 196). The potential problem with using this approach should be readily evident. The amount of information a smart phone can contain far exceeds that which a conventional cellular phone can hold. Today's cellular phones are even more powerful and have greater potential than older computers.

Orso questions whether courts should allow officers to continue searching phones incident to arrest as some courts have found to be permissible given that they have "generally reasoned that a cellular phone differs little from a basic pager, address book, or cigarette box, all which may be lawfully searched incident to a suspect's arrest" (2010, 201). To adopt this stance with respect to smart phones would "subject anyone who is the subject of a custodial arrest, even for a traffic violation, to a pre-approved foray into a

virtual warehouse of their most intimate communications and photographs without probable cause" (Orso 2010, 211). Based on the few cases involving laptop and computer searches incident to arrest as well as the similarity that smartphones have with laptops Orso reasons that "if it is true that laptops and other computers are not searchable incident to arrest, then it necessarily follows that neither are smart phones (or at least they should not be)" (2010, 219). Orso's proposed solution is then to differentiate between the type of cellular phones in question and to apply different standards when determining whether a search incident to arrested is allowed for each.

Engel's works supports Orso's to a great extent. He too notes that the majority of lower courts have "concluded that the content of cell phones may be searched incident to arrest without limitation" (Engel 2010, 253). He further points out that newer model cellular phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures" (Engel 2010, 257). With respect to searches incident to arrest Engle notes that "the ability of electronic devices to store information is changing rapidly, and it is foolish consistency to continue to try to place the square pegs of electronic devices in the round hole of the container doctrine" (2010, 292). He cautions, however, that such a claim is not meant to "suggest that the entire search incident to arrest doctrine should be abandoned or even re-examined" (Engle 2010, 292). Engle too finds the more appropriate solutions would be to merely differentiate between the types of devices that would fall under already existing standards. Engle and Orso's works further emphasizes the import of more clearly defining the relationship between the law and the internet since the outcome in this relationship could impact future technological innovations.

The ever-evolving changes in technology, of which Orso and Engle used smart phones as an example, and the problems it may pose on the Fourth Amendment is expanded upon by Strandburg (2011). The growth of social media and cloud computing, Strandburg posits, "will make it impossible to preserve the privacy even of traditional Fourth Amendment bastions, such as the home, without considering the intertwined effects of technological and social change" (2011, 106). The argument she presents runs counter to those that may think that the internet is its own space. On the contrary, she claims, the internet has advanced to a point where past Fourth Amendment rulings "will be insufficient if we hope to extend meaningful Fourth Amendment protection into a networked world in which technology and social behavior are co-evolving" (Strandburg 2011, 108).

A large concern that Strandburg has about the future of the Fourth Amendment in the new technological realm lies in the reliance on the third party doctrine upon which previous Fourth Amendment cases such as *Miller* and *Smith* have relied. The third party doctrine "in which every activity involving a digital intermediary is open to law enforcement scrutiny (at least as far as the Constitution is concerned)" will become more troublesome with respect to Fourth Amendment protection "in the whole range of social contexts making up the integrated online-offline world" (Strandburg 2011, 127-128). As cloud computing gains popularity and more and more people store personal information online these actions will raise questions such as whether the service providers that store this information count as third parties that may be approached by officials and asked for information.

The solution that Strandburg proposes for the potential Fourth Amendment questions that may arise from the increasingly intertwined relationship people may have with the internet is not to create a wholly new standard, however, but rather to extend upon previous Fourth Amendment standards. More specifically she links the new innovations to physical ones, nothing that "just like hotel and guest rooms, cloud computing arrangements and social media of various kinds share many (but not all) of the attributes that motivate strong Fourth Amendment protection of the home and office" (Strandburg 2011, 145). Strandburg considers that "these technologies are potentially the technosocial extension of our homes and offices and, like hotel rooms and curtilages, need Fourth Amendment protection" (2011, 145). Yet Strandburg, as other scholars have noted, identifies the difficulty of addressing these issues nothing that "while courts are still grappling with text messaging and e-mail, society has moved on, integrating the web more and more seamlessly into the social realm and providing virtual extension of the home, the office, and other core loci of private life" (2011, 164). Strandburg's work can ultimately be said to stand somewhere in the middle of the internet regulability debate. On the one hand it seems she does not feel all old Fourth Amendment principles are amenable to the internet as it evolves, as is evident from her suggestion to place less emphasis on the third party principle. On the other hand she acknowledges the new areas created by these new internet technologies do require Fourth Amendment protection and the manner in which she proposes that this be accomplished is by granting them similar protection to physical locations, such as hotel and guest rooms.

The question then being posed here, asking how the Fourth Amendment is interacting with the internet may then offer some insight in the debate between those that

favor regulation of cyberspace and those that are wary of the ability to easily do so. It may also reveal how courts are reacting to the problems that many of the authors noted above have observed such as the adequacy of applying real world traits to cyberspace. Though any findings presented here will far from settle this debate they may nevertheless clarify the issue. Constancy in the manner in which courts treat Fourth Amendment issues even in the wildly new frontier of the internet would bolster the case for those favoring regulation given that such a finding may indicate the structural barriers posed by the internet are not as unassailable as the skeptics may claim. On the other hand, finding inconsistent rulings may reveal that the law on the internet is more mercurial than some may expect, and may indeed pose an obstacle for regulation and a new conceptualization of the relationship between the law and cyberspace may be needed.

Given that at issue here is how courts treat Fourth Amendment questions involving the internet the most evident approach is to examine relevant cases from appellate courts, with Supreme Court cases being the most preferable, in which Fourth Amendment violations committed online in some form are called into question in prosecutions. By examining the reasoning given in the opinions of these cases it can be determined if courts remain loyal to the guidelines that resulted from *Katz*. Ultimately the nature of the crime itself is not wholly relevant given that the main concern is whether courts exhibit a consistency of reasoning not just among cyberspace cases but also with older cases involving other technological innovations. Undoubtedly, however, cases with real-world analogues may be particularly useful in tracing the similarity of reasoning, or lack thereof. It would then be preferable to consider cases wherein the expectation privacy of an individual online is called into question. *Warshak v. United States* would be

an example of a suitable case to study for the purposes presented here. The case calls into question whether the police violated an individual's Fourth Amendment rights when they made his Internet Service Provider hand over his e-mail without a search warrant. Such a case would directly address the type of problem Kerr (2003) with respect to internal or external perspectives taken by the court.

Cases such as *Warshak* would need to have their reasoning scrutinized and compared to past high profile Fourth Amendment cases involving other forms of technological innovations, such as *Smith* as noted above, to determine if the fundamental lines of reasoning between the various chosen cases remain consistent. A secondary aim when considering cases may also specifically address the type of complaint that Bomse described relating to the adaptability of the law to the internet. This phenomenon may be examined by following a case along the appeals process and determining if some reaction to a cyber-related evolution altered the reasoning process between the different courts. Such an analysis would be secondary to the main goal, however.

To support the methodological approach outlined above it may help noting other articles that draw parallels between cyber-world and real-world acts. In "Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication" (1997), parallels are drawn indicating how acts on the internet can be seen as analogues of real-world cases where the Fourth Amendment may come into play. E-mail, for example, can be seen as analogous to traditional mail or even communication via the telephone, which is an act that was directly addressed under the Fourth Amendment in *Olmstead v. United States* (Anon. 1997, 1597-1598). If a case were to arise that were comparable to *Olmstead* but set in cyberspace, one may then expect a similar decision.

Yet, as will be noted, even if similar cases have different outcomes it may not necessarily be true that the reason behind it is due to an evaluation on fundamentally different principles.

In "The Developments in the Law: The Law of Cyberspace," (1999) it is noted that a similar approach has been undertaken to examine the relationship between the law and the internet. The article cites a case wherein plaintiffs were awarded damages by a federal jury over a speech related matter on the internet even though a federal judge had previously enjoined the enforcement of a law that would have restricted the type of speech in question (Anon. 1999, 1582). From this case the author suggests that perhaps "the bounds of permissible regulation of Internet speech derive directly from established, real-space First Amendment jurisprudence, under which governmental attempts to regulate speech content are normally subject to strict scrutiny" yet those that still feel they have been wronged may "pursue each other in actions for libel, defamation, and death threats" (Anon. 1999, 1582). The on-line case then seems to parallel a real-world scenario where it may be very difficult to stop certain forms of speech, yet people still have a recourse if they feel aggrieved. To find a relationship such as this, but relating to the Fourth Amendment, wherein real-world principles carry on to the Internet would then further bolster the claim made in this article. This article also alludes to the larger reach that the relationship between the law and the internet may have on other individuals, noting about legal rules that "not only will these rules affect people's cyber-lives, but because cyberspace life is becoming more entwined with real-space life, the rules governing virtual communities will also influence our real-space communities" (Anon.

1999, 1587). Such a claim once again emphasizes the potential impact the relationship between the law and the internet may have.

The parallel between the real world and cyberspace is not absolute, however, given that "exception for searches incident to a lawful arrest, necessary to protect life, in hot pursuit, under exigent circumstances, and at the U.S. border will rarely be relevant to investigations of cyber-communications" (Anon. 1997, 1599-1600). But as scholars such as Orso (2010) and Engel (2010) have noted above even this line has become more blurred with the advent of smartphones. Yet there still remain other exceptions that may still come into play such as "when consent to search has been given, when the information has been disclosed to a third party, and when the information is in plain view of an officer" (Anon. 1997, 1600). This comparability illustrates that the potential for conflict between the Fourth Amendment and the internet is rather large. Taking e-mail alone for example once again, someone may believe their e-mails are to remain private if they were to be transmitting questionable material but a systems administrator may notice the interaction and alert authorities. In the internet there are many third parties such as a systems administrators, service providers, or even hackers that could come across information one expects to be private and then make it public, meaning there are potentially many points of friction between the Fourth Amendment and the internet.

As touched upon briefly before, caution must be used when examining the reasoning behind relevant cases, though, even if the facts of the cases appear to be similar to their real-world equivalents. This is the case because even in past Fourth Amendment cases that appeared to have been similar different courts arrived at different opinions. This does not mean that one court followed the *Katz* standard while another disregarded it

either partially or completely, however. On the contrary, in cases such as these all courts in question will likely claim that they remained loyal to *Katz*. The differences between the decisions in these instances lies in the particular details each court chose to emphasize in each. It is therefore possible for similar cases to arrive at different conclusions, yet still follow the same fundamental framework. Therefore the cases used to evaluate the relationship at issue here cannot have the reasoning scrutinized too harshly against previous cases. If a pair internet related cases, for example, were both relatively analogous to a real-world case yet courts rule in opposite ways for each this does not necessarily invalidate the cases from consideration, the difference in decision would instead simply have to be justified by the slight differences in reasoning used by each court. It is the fundamental principles behind the reasoning that are most poignant.

The type of situation alluded to above is addressed by Sergent (1995) and his work emphasizes the idea that small factors could lead to differing opinions between similar cases. His work demonstrates that the methodological approach taken here does not need to have perfect correspondence between real-world and cyber-world cases. Sergent outlines the problems that have arisen from the relatively subjective test that resulted from Justice Harlan's *Katz* concurrence and considers how these problems may affect computer networks. He delves deeper into one aspect of the *Katz* test, this being the expectation of privacy, and illustrates how determining this key factor may vary greatly depending on "ownership of the computer, ownership of the information involved, and control of or access to the computer and information" (1995, 1195). Sergent's observations emphasize that although the small idiosyncrasies of each case ultimately will not be the focal point of the case studies it may nevertheless be fruitful to

consider whether courts' decisions hinge on comparable points of contention as they did in the cases of previous technological innovations. To find that the same types of details are often critical in deciding these types of Fourth Amendment cases as were critical in previous ones, may strengthen the connection between the technologies even though on their face the cases may not seem all too comparable. Furthermore it should be noted that these types of subjective judgment calls exist even in old Fourth Amendment cases.

A hypothetical example regarding the difference between evaluating the reasoning versus the outcome of court decisions that is surely likely to have played out in the real world may revolve around the physical location of a criminal action. Two cases with otherwise very similar characteristics could nevertheless have potentially different outcomes merely because one defendant was working on their personal computer at home whereas another was working in an office they shared with other people on their company's computer. If a third party were to find questionable material they obtained from the internet on their computers then informed the police who proceeded to search their computers without a warrant then both courts could potentially apply the Katz test with varying outcomes. It could be argued that the person at home had a greater expectation of privacy and where the search would be invalid in that case it would still be valid in the case where the person's computer was in their workplace. Though these cases could end up with opposite decisions with respect to the warrantless searches the courts nevertheless applied the same fundamental principle. By inquiring about the reasoning used in cases rather than the actual outcomes one may therefore be able to ascertain more substantial results with respect to how courts are treating internet related cases. One judging merely based on the outcome may infer that courts are wildly inconsistent in how

they handle internet cases when in fact they may be using the same reasoning and are actually being very consistent in their approach. This example uses rather large differences between two cases but other cases could have an innumerable amount of minor details that could affect the outcome while the reasoning nevertheless remains the same.

Even if cases have highly varying outcomes they are still likely to be relevant for the purposes presented here. The extent to which courts remain faithful to the reasoning in previous cases dealing with other technological innovations and the Fourth Amendment could be interpreted as a matter of degree, from a strict adherence to the past to a large break with traditional reasoning. A result anywhere along this spectrum is likely to signify a different outcome in the relationship between the law and the internet. The implications of this work then, as has also been touched upon above, is therefore much larger in scope than the actual question at issue.

The subsequent chapters of this work will be organized with the methodology outlined next, followed by the results chapter, and then concluded with the discussion chapter. The methodology chapter will expand upon the basic outline presented above as well as address how cases will be selected. Furthermore this chapter will address potential benefits as well as problems that may arise from using a comparative approach. The findings chapter will consist of the court cases chosen for the inquest, and will outline the overall facts of the case. The reasoning used in the courts' opinions will be examined for potential trends or other significant findings in their reasoning, such as the emergence of new principles on which internet cases are judged. In the discussion section the greater significance of the findings will be examined. This final section will

also attempt to integrate the findings into the debate outlined above concerning the ability to regulate the internet.

The internet has truly been a revolutionary innovation that may have been hard to imagine merely decades ago. It is obvious, though, that courts have had to deal with large technological innovations before as well when they interacted somehow with the Fourth Amendment. The internet's impact on the lives of most people can make it arguably one of the larger technological innovations that the court has dealt with, however. It may be too bold a statement, though, to claim that the law must start from a clean slate when it is considered in the context of the internet. Similarly to claim that decades-old principles can be easily transplanted to function when considering legal issues online may be too simplistic a claim as well. The various cases that courts have previously considered are likely to serve as a more than adequate foundation when it comes to addressing at least some fundamental issues that come up when the internet and the Fourth Amendment come into contact. This relationship may then in turn help shed some light on the larger relationship between the law in general on the internet.

Chapter 2: Methodology

The issue to be addressed pertains to the way that U.S. courts have reacted to Fourth Amendment conflicts on the internet. This question is but a smaller subset of the much larger issue concerning the relationship between the law and its adaptability in the age of the internet. The main goal of this inquiry is to determine whether courts have been consistent in regards to how they handle Fourth Amendment issues online when compared to how they have handled these issues when they involved other technological innovations. On the one hand it is possible that the internet is treated just as any other technological innovation has been treated and on the other it could be that it is such a different type of technological innovation that a wholly new point of view must be taken when dealing with the issues that arise with it. A third alternate outcome may even be that some half-way adaptation has occurred; building upon the old foundations that were used to deal with previous Fourth Amendment issues but also creating new principles to address internet-specific problems. The hope is that by looking into this issue a better understanding of the path that courts have taken in interpreting the Fourth Amendment with respect to the internet can be achieved and furthermore this knowledge may lend some insight into the relationship between the law and the internet in a more general sense.

A broad description of the methodological approach to be taken will first be outlined before then going into more detail with respect to the process. Afterwards potential difficulties that this approach may give rise to will be addressed. A general description of the particular methodology that will be used to address the issue in question is that it will be done comparatively. Cases that demonstrate the Fourth

Amendment clashing with some sort of technological innovation will be compared to Fourth amendment cases involving the internet. This comparison will be done by examining the reasoning between the various cases that are relevant to the issue and determining whether or not it is consistent as well as whether new principles have been adopted to deal with specific internet-related issues.

Having given a general overview of the methodology that will be used a more detailed view is now required. The facts of the cases that are chosen will presented and their opinions will be analyzed and their reasoning will be compared to that of relevant high profile cases that have dealt with the Fourth Amendment problems raised due to past technological innovations. The types of cases that are chosen need not be analogous to each other, on the contrary greater diversity between the kinds of cases could arguably yield more robust results. If the reasoning remains consistent between wildly varying cases, including those involving the internet, this would suggest that the internet may be amenable, at least to a degree, to previously established principles.

Gathering useable cases is a relatively simple process, seeing as the elements used for comparison will be actual court opinions. The availability of these sources should not be a large impediment; the more difficult part will be determining which cases are and are not relevant. The internet will itself be a valuable resource in gathering information given that many courts have their opinions digitized and made available online; more specifically the online database LexisNexis will likely be an unparalleled source for gathering actual case opinions. Furthermore the more influential cases, such as *Katz v. United States* for example, are more likely to be readily accessible on the internet. Therefore finding the most influential cases involving technological innovations of all

sorts should not be as daunting a task as one may first expect. To only use the most widely known cases may yield a sample size that is too small and potentially biased given that their fame may be due to a controversial ruling based on reasoning most other courts would not have employed. So for gathering a larger number of relevant cases a brute-force approach may be the tactic that reveals the largest amount of potential candidates. Such an approach would require searching for any cases involving internet related actions which would then be filtered based on the facts to reveal those that addressed Fourth Amendment issues.

The process for determining the potential pool for relevant cases relies on a few factors. The cases obviously need to raise a Fourth Amendment claim. To add some refinement to the potential pool of cases as well as more significant findings, given that their opinion carries more weight, district court opinions will be bypassed in favor of appellate court opinions. The pool of potential cases will be further refined given that several claims can be made with respect to the Fourth Amendment; such as questions about probable cause or questions regarding the scope or legitimacy of warrants. In order to be able to more readily isolate and compare reasoning patterns between cases it would then be more beneficial to focus on one particular Fourth Amendment issue raised in the chosen cases. For instance one would not expect to be able to compare reasoning between one case that questioned the presence of probable cause on the one hand and one arguing an overbroad warrant on the other. For this reason the cases examined here will include the question of whether a warrantless search was justified under the Fourth Amendment.

The cases found to be relevant to the issue at hand can then have their opinions scrutinized. The reasoning given for deciding the particular Fourth Amendment issue in

question in each case can then be gauged against previous cases. The most general comparison being made could be to *Katz v. United States*, which has been the foundation for current Fourth Amendment jurisprudence regarding one's legitimate expectation of privacy. Other cases may also be relevant, however, if the particular facts of the cases appear to be analogues of each other. Additionally, other cases have built upon *Katz* so it is quite likely that the reasoning used in these may also be relevant when comparing cases. Opinions often explicitly indicate what previous cases they are basing their decisions on, further making finding worthy cases for comparison convenient. The comparison must still be made, however, to ensure whether or not the reasoning remained consistent. Furthermore as one would expect if a principle were to be created due to address an issue unique to the internet then one can hardly expect a reference to a previous case.

With respect to more specific mapping of the reasoning used in cases one approach would be searching, for instance, whether the case applies the reasonable expectation of privacy test that is laid out in *Katz*. So both objective and subjective expectations of privacy will be key words when determining if and how the Katz test is applied. By examining whether or not courts apply this test as well as how they interpret the different expectations of privacy in a wholly new environment can speak to the ability of older principles to survive or be adapted when it comes to the internet. Given the importance the reasonable expectation of privacy test has had in Fourth Amendment cases it makes sense to use it as the backbone for comparison within cases. To find that a case abandons this test would signify a substantial departure from past principles. A second principle that may be important to look for would be the third party principle.

Though this principle is not explicitly mentioned in *Katz* it can come up in when considering the question of an expectation of privacy given that the principle claims one does not have an expectation of privacy with respect to information exposed to a third party. Perhaps this principle may come into play more often than usual on the internet since individuals may have more of a proclivity to think that they are anonymous online.

As has been noted it is the reasoning that will be scrutinized of any case that is taken into consideration. Therefore there will be a consistency in methodology throughout the older cases used for comparison and the newer ones. Along with this consistency of approach this methodology further has the benefit of objectivity given that by their nature opinions are meant to be clear and easily understandable. This approach, therefore, should result in an accurate, first-hand, mapping of the way courts have or have not adapted to the internet with respect to Fourth Amendment cases. By comparing the reasoning used in internet-related cases to those involving other technological innovations it can be determined whether the internet is being treated as other technological innovations were. For instance if it is found that there is consistently a new type of reasoning utilized that is not found in older cases, then this may be indicative of the truly revolutionary nature of cyberspace under which previous methods are not applicable. Conversely to find a consistency in reasoning techniques between other technology types and the internet-related cases may indicate that cyberspace, though a much larger technological innovation, is still amenable to the old real-world techniques.

Perhaps the biggest potential problem that faces this type of research is a dearth of viable cases from which to draw upon. Given the pervasiveness of the internet, however, at least some high profile Fourth Amendment cases should be expected. With people

performing crimes online it should be expected that law enforcement may at times be faced with Fourth Amendment questions in the course of performing their duties. The availability of potentially useful cases is undoubtedly most troublesome with respect to cases addressed by the Supreme Court. For this reason it would then be more prudent to include lower court rulings into the potential pool of cases taken into consideration. As has been noted, to add some refinement to the potential pool the field of potential cases will be reduced by considering only appellate court cases. Such an approach would have the benefit of providing a larger pool than merely Supreme Court cases while also ensuring that the more potentially controversial cases are taken into account.

The method used to gather useable cases also poses some difficulties. Given that it consists of poring over cases one at a time to determine whether they may or may not be relevant one cannot expect to include every potentially useful case. There is a danger, therefore, that a few particularly important and relevant cases may be overlooked in the selection process. Gathering a respectable amount of sample cases though may aid in remedying or at least minimizing the impact of this potential problem.

Another potential problem with conducting this type of research deals with consistency and is closely tied to the problem of the paucity of useable cases. Given that the internet is such a relatively new innovation it is understandable that courts may still be grappling with how to react to it. As a result of the novelty of the technology one may then fear that courts may not have harmonized yet as to how to address the cases that arise. How can one expect perfect harmony when the issue being considered may not contain a real-world analogue close enough to base a decision on? When taken in the context of the purpose of this work this potential characteristic does not necessarily have

to pose an impediment. On the contrary, harmony or a lack there-of within the courts would in and of itself be informative given that the reasoning in these instances could be parsed to determine whether or not it still relies on the same fundamental principles as the older cases.

The case selection for the purposes outlined here requires two general types of cases to be gathered. First there needs to be a basis for comparison. This will be manifested by a selection of cases that display a conflict between the Fourth Amendment and some form of technological innovation that is not the internet. As noted, the specific issue in question will be whether or not a warrantless search is considered valid under the Fourth Amendment. The case of *Katz v. United States* will essentially be the baseline upon which the remaining cases will be compared given the prominence it holds in Fourth Amendment jurisprudence. The other cases used for comparison will then be examined to determine whether they too follow the rationale as presented in *Katz* when determining the validity of a warrantless search and if they do then how do they go about doing so.

The second type of case that is needed for the purposes presented here will consists of cases in which the Fourth Amendment conflicts in some manner with the internet. Given that the internet can be used for various functions, such as communication or transferring information, many of which could potentially be illegal, this aspect combined with its potential of allowing third parties to access these transactions means occasional run-ins with the Fourth Amendment can be expected. As previously described the specific type of Fourth Amendment question that will be examined in these cases is whether a warrantless search can be deemed valid. The manner in which the internet-

related question go about determining this issue will then be compared to how it was done in the pre-internet cases. Trends or differences between the pre-internet and internet cases can then hopefully be more readily identified. Furthermore emerging principles may be identified if the reasoning between the two main groups is found to shift.

The result obtained from conducting this research could then be used in conjunction with other works, for instance work examining the relationship between the internet and the First Amendment, to lend some insight into the question pertaining to the degree to which the internet can be regulated or if it can be regulated at all. Regardless of the actual findings the results are sure to add another piece to the larger puzzle that represents the relationship between the law and the internet. Seeing as how more and more aspects of every-day real-world life are becoming merged with the internet the import of better understanding this relationship is readily evident.

Chapter 3: Results

As has been mentioned before the manner in which the relationship between the Fourth Amendment and the internet will be examined will be by considering how cases involving the Fourth Amendment and the internet are treated by the court when considered vis-à-vis the reasoning used by the court in other Fourth Amendment cases involving technology. The case of *Katz v. United States* (389 U.S. 347, 1967) will function as the baseline case upon which remaining cases will be examined. The reason behind this is because *Katz* established the reasonable expectation of privacy test that courts use to determine whether a person holds a legitimate expectation of privacy under the Fourth Amendment with respect to the object or items seized or searched that may then invalidate that search. Subsequent cases can then be considered to determine whether they followed the reasoning in *Katz* in determining whether the warrantless searches in their situations were valid or not. The case studies will be presented here in chronological order in order to more easily identify trends, or the lack thereof, throughout the various technologies. Other pre-internet cases involving some form of technology will first be examined to determine how they compare to *Katz*. Finally internet-related cases will be examined to evaluate whether the reasoning used by the courts was consistent.

Non-Internet Cases

The first and most fundamental case that must be examined for the purposes presented here is *Katz v. United States* (389 U.S. 347, 1967). The precedent established by this case will be followed to determine whether it still holds in the age of the internet. In this case Charles Katz was recorded by an electronic eavesdropping device, without

having first gotten a warrant, placed outside a public phone booth. He was using the phone to place illegal gambling bets. Katz was convicted because of the recordings and appealed his conviction, claiming the recordings violated his Fourth Amendment rights. The Court of Appeals affirmed Katz's conviction. Ultimately, however, the Supreme Court granted certiorari and ruled in Katz's favor.

This case is suited as one of the cases for comparison because not only is it a landmark case with respect to the Fourth Amendment but it also deals with the conflict between the Fourth Amendment and technology. The Court addressed whether a search required a physical intrusion to take place, given that Katz was not physically searched by police officers. Furthermore the Court asked whether a telephone booth is a location under which one can expect a right to privacy. These questions are deemed key by the court when determining whether a search without a warrant is valid under the Fourth Amendment.

The case of *Katz v. United States* established the expectation of privacy test. This test helps determine whether a warrantless search is justified under the Fourth Amendment. It was justice Harlan's concurrence that created the test now employed in these types of cases. Justice Harlan summarized the Court's opinion to mean

> (a) that an enclosed telephone booth is an area where, like a home, *Weeks* v. *United States*, 232 U.S. 383, and unlike a field, *Hester* v. *United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area

> by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant. (*Katz v. United States* 1967, 360-361)

Justice Harlan then outlined a test in which there are two elements that must be demonstrated in order for someone to claim a legitimate expectation of privacy under the Fourth Amendment. These elements are "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'" (*Katz v. United States* 1967, 361). To find that the application of this test persist throughout different technologies as well as the internet would indicate that the internet may be amenable to a degree to current laws, meaning it is not necessarily a "no man's land" in the eyes of the law.

When deciding the issue in question in *Katz* the Court stated that the "Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and this constituted a 'search and seizure' within the meaning of the Fourth Amendment" (*Katz v. United States* 1967, 353). According to the Court Katz's expectation of privacy when entering a phone booth was both subjectively and objectively reasonable given that with respect to phone booths; "one who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world" (*Katz v. United States* 1967, 352). After *Katz* other kinds of technological innovations also came under scrutiny when it came to the Fourth Amendment.

Following *Katz* the Court once again looked at the implications of technology on the Fourth Amendment in *Smith v. Maryland* (442 U.S. 735, 1979). In this case Michael Smith kept calling the house of a woman he had robbed. Based on information given to them by the woman the police identified his car and by tracing his license plate found his address. The police then asked the telephone company to install a pen register in order to record the phone numbers dialed from Smith's home. A pen register is an electronic device that records the dialed numbers from a specified phone line. Based on the installation gathered from this pen register the police confirmed that Smith was indeed calling his victim and then charged him with robbery. Smith argued that the use of the pen register constituted an illegal search as understood by the Fourth Amendment. Similarly to *Katz* the Court had to determine whether the use of this piece of technology could truly be considered a search under the Fourth Amendment.

The Court argued that "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action" (*Smith v. Maryland* 1979, 740). The Court agreed with the *Katz* Court when it found that to determine whether the Fourth Amendment protection extends to a claim of this kind that the test outlined in *Katz* was adequate. Unlike the *Katz* Court, the *Smith* Court did not believe that the use of a pen register constituted a "search" given that its use did not violate Smith's reasonable expectation of privacy. The Court first claimed it they did not believe people generally hold an expectation of privacy with respect to the phone numbers they dial. The reason behind this being that "all telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone

company switching equipment that their calls are completed" (*Smith v. Maryland* 1979, 742). Furthermore the Court noted that the location from which the phone number was dialed was immaterial, even if it is from the privacy one one's own house, given that "regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call" (*Smith v. Maryland* 1979, 743). Therefore the court concluded one could not hold a reasonable subjective expectation of privacy when dialing numbers on their phone.

With respect to the second prong of the test the Court reiterated that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (*Smith v. Maryland* 1979, 743-744). Therefore "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business" *(Smith v. Maryland* 1979, 744). The Court reasoned then that when one dials numbers on the telephone these numbers are essentially being transmitted to a third party, meaning the phone company, in doing so the dialers assume the risk of those numbers being given up to the police by the telephone company. Given this dynamic the Court argued that one cannot claim that society would recognize such a willing conveyance of information as compatible with an expectation of privacy. Therefore taking these two findings the Court concluded that Smith "entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate'" so the use of the pen register "was not a 'search,' and no warrant was required" (*Smith v. Maryland* 1979, 745-746).

Whereas *Katz* and *Smith* involved technological innovations more specifically designed for the purposes of gathering information in *California v. Ciraolo* (476 U.S. 207, 1986) a different kind of innovation was scrutinized. The issue addressed in *California v. Ciraolo* involved the implications of the Fourth Amendment when it came to aerial observation. Police received an anonymous tip wherein the caller told them Dante Ciraolo was growing marijuana in his backyard. A fence shielded the crop from observation at ground level. Officers flew in a private plane over the area and were able to confirm that there was a marijuana crop in the backyard. A search warrant was obtained based on these officer's actions. Ciraolo pleaded guilty of marijuana cultivation after the trial court refused to suppress the evidence. The Court of Appeals, however, reversed the decision. This decision was ultimately reversed once again by the Supreme Court. The type of technology in question is the aerial surveillance that granted the police the ability to observe activity they otherwise may not have seen. The Court had to determine whether the type of surveillance made possible by using the plane was valid without a warrant.

Once again the Court's reasoning in this case revolved around the *Katz* test. With respect to Ciraolo's subjective expectation of privacy the Court noted he "met the test of manifesting his own subjective intent and desire to maintain privacy as to his unlawful agricultural pursuits" given that he constructed a 10 foot fence around his marijuana crop(*California v. Ciraolo* 1986, 211). With respect to the second portion of the test the Court argued that even though Ciraolo had erected the fence "any member of the public flying in this airspace who glanced down could have seen everything that [the] officers observed" (*California v. Ciraolo* 1876, 213-214). Ciraolo could therefore not claim he

had a reasonable expectation of privacy given that though he had a valid subjective expectation of privacy, he did not have a valid objective one. The Court concluded that the "Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye" (*California v. Ciraolo* 1876, 215).

The case of *United States v. Meriwether* (917 F.2d 955, 1990) presents a few interesting findings with respect to how the court viewed technological changes. Upon executing a search warrant DEA agents found a pager belonging to one of two men arrested on the scene. The agents monitored the pager and recorded several of the phone numbers that sent messages to it. One number that appeared repeatedly was chosen at random and was called by an agent. The man who answered was Chester Meriwether and he set up a meeting with the agent, who was pretending to be someone else, where he would buy $4,800 worth of cocaine. The agents showed up to the meeting and arrested Meriwether. Meriwether attempted to have all the evidence related to the phone conversations suppressed but was denied. On appeal the court was faced with answering the question of whether Meriwether's Fourth Amendment rights were violated when the agents attained his phone number from the pager. Even though the agents in this case had a search warrant this case is still acceptable for the purposes presented here because the court explicitly asks whether the search of the pager would still have been valid had the search warrant not included the contents of the pager. It is this specific portion of the case that will be scrutinized.

This case's reasoning is significant for two reasons; one being that it presents a kind of reasoning that speaks to the ever evolving way in which information is stored

through technological means. Second the court once again applied the reasonable expectation of privacy test to yet another type of technological innovation. In *Meriwether* the court agreed with the lower court's claim that retrieving a number from a pager is akin to retrieving a number from someone's personal telephone book, noting that "the digital display pager, by its very nature, is nothing more than a contemporary receptacle for telephone numbers" (*United States v. Meriwether* 1990, 958). This claim by the court is supported by the arguments made in *United States v. Reyes* (798 F.2d 380, 1986) where, in questioning how specific a warrant needed to be, that court noted "in the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form records could take" (*United States v. Reyes* 1986, 383). The court concluded that the warrant in question in *Meriwether* was broad enough to allow the pager numbers to be looked at. The implications of the court's reasoning here may then be especially significant in the age of computers given that they serve a wide array of purposes. For instance computers by themselves could be seen as akin to file cabinets storing a wide array of files furthermore in the age of the internet with the advent of programs such as Skype computers can also function similarly to telephones that also store contact information of many individuals.

Though the court found the warrant in question to be valid in this case, it went beyond this and questioned if the Fourth Amendment claim made by the appellant would still carry weight had the warrant not been valid. The court reasoned that in *Katz* the defendant was justified in his expectation of privacy in the phone booth so the actions taken by the police in that case were accurately considered a search and seizure. To

determine whether the information gathered from the pager constituted a search and seizure in this case the court applied the Katz test. The court argued that when someone sends a message to a pager they have no real way of knowing who will be on the receiving end of that message; it could be the intended recipient or a police officer that has just arrested that intended recipient. So he failed "to show that he sought to preserve a message as private by transmitting it into a paging receiver over which he [had] no control" (*United States v. Meriwether* 1990, 959). He therefore could not claim an expectation of privacy given he had no certainty as to who would receive his messages, so the actions by the police did not qualify as a search and seizure. So had the warrant not been valid the court still would not have considered that the appellant's Fourth Amendment rights were violated.

The following two cases, the first being *United States v. Pinson* (24 F.3d 1056, 1994), are significant because both employed the *Katz* rationale but they were later overturned by a third case that did not. The case of *United States v. Pinson* dealt with yet another technological innovation that raised Fourth Amendment questions. The case involved an infrared device that was able to detect heat emanating from a structure. Police learned that Joseph Pinson's house had received packages from known suppliers of hydroponic growing equipment. They also subpoenaed the utility records for Pinson's residence as well as those of some other nearby residences. The records indicated a large amount of electrical usage by Pinson's residence which the police claimed was indicative of the amount needed to maintain an indoor marijuana crop. Based on this information the police mounted a Forward Looking Infrared Device (FLIR) onto a police helicopter an flew over Pinson's residence. The device revealed a large amount of heat emanating

from a covered window, the roof, and a skylight of the residence. Using this information the police obtained a search warrant and found an indoor marijuana growing operation in the third floor of Pinson's residence. Pinson claimed that the observation of his residence with the FLIR violated his Fourth Amendment rights given that it was conducted prior to the police attaining a search warrant.

The court claimed that "a party claiming to have suffered an unlawful invasion in violation of the Fourth Amendment must establish as a threshold matter that he had a legitimate expectation of privacy in the object searched or seized" (*United States v. Pinson* 1994, 1058). To determine whether a legitimate expectation of privacy was present the court turned to the Katz test. With respect to the question of a subjective expectation of privacy in this case the court found the escaping heat from the structure to be comparable to discarded garbage. Given that discarded garbage had previously been found to not be worthy of a subjective expectation of privacy the court reasoned that in this case there was "no reasonable expectation of privacy in heat which Pinson voluntarily vented outside" (*United States v. Pinson* 1994, 1058). With respect to the objective expectation of privacy the court once again employed an analogy declaring the use of an infrared device "analogous to the warrantless use of police dogs trained to sniff and identify the presence of drugs" and expanding on this noting that "just as odor escapes a compartment or building and is detected by the sense-enhancing instrument of a canine sniff, so also does heat escape a home and is detected by the sense-enhancing infrared camera" (*United States v. Pinson* 1994, 1058). Claiming an expectation of privacy against the use of the infrared sensors in this case failed both portions of the Katz

test, so Pinson's claim that the warrantless search by using the infrared device violated his Fourth Amendment rights was denied

A thermal imager was under scrutiny once again in *United States v. Ford* (34 F.3d 992, 1994) and it was handled using the same fundamental principle. After receiving information that Jerry Ford and Dorothy Ford Longmire were growing marijuana inside a mobile home police officers set up surveillance outside the home. Using a thermal imager they detected a large amount of heat emanating from the trailer's floor and walls. The heat was consistent with the kind emitted from other indoor growing operations. This information contributed partly to the police obtaining a search warrant for the mobile home. Ford had boarded up the windows to prevent light from escaping and had also created holes in the floor supplemented by blowers in order to vent the excess heat created by the lights. Ford, like Pinson, argued the use of the thermal imager constituted an illegal search under the Fourth Amendment.

The court noted that it had to decide whether the use of the imager constituted a search under the Fourth Amendment. To answer this it noted that "the touchstone for this decision is whether the alleged search violated the defendant's legitimate expectations of privacy" (*United States v.* Ford 1994, 995). Once again the court attempted to answer this question by establishing whether Ford satisfied the Katz test. With respect to his subjective expectation of privacy the court noted that "while Ford was careful to prevent any light from escaping the mobile home – for example, by boarding the windows from the inside -- he took affirmative steps to vent the excess heat that was detected by the FDLE's thermal imager" (*United States v. Ford* 1994, 995). So while he tried to keep the extra light he created secret, he actively tried to vent the extra heat from his home. Given

this behavior the court argued that Ford "did not seek to preserve the fact of that heat as private" so he could not claim a subjective expectation of privacy with respect to what the heat the imager detected (*United States v. Ford* 1994, 995).

With respect to Ford's objective expectation of privacy the court compared the thermal imager to aerial observation, claiming that like aerial observation the thermal imager was not powerful enough to actually reveal "the intimacy of detail and activity protected by the Fourth Amendment" (*United States v. Ford* 1994, 996). The court went beyond this, however, and once again compared the heat emanating from the house to discarded waste, which had previously been found to not possess an objectively reasonable expectation of privacy. Furthermore, even though the elements that Ford exposed were not visible to a normal passerby, the court referred to aerial observation and drug sniffing dogs to illustrate that tools used to enhance the senses do not necessarily render an instance of surveillance as unreasonable under the Fourth Amendment.

The third and perhaps more significant case involving a thermal imager to be examined here is *Kyllo v. United States* (533 U.S. 27, 2001). The reason that this is of particular interest for the purposes presented here is that unlike the previous two cases involving thermal imagers that upheld their use without a warrant, this one invalidated the use of an imager without a warrant. In this case after a United States Department of the Interior agent suspected that marijuana was being grown in the home of Danny Kyllo he used a thermal imager to scan the home. The agent was aware that indoor growing operations required high-intensity lamps which would create a heat signature that the imager could detect from the outside. The agent's scan with the imager took only a few

minutes and was conducted from both the street in front of the house and the street behind the house. The results of the scan indicated that certain parts of the home were relatively hot when compared to other parts and that the home itself was also hotter than the surrounding homes. From the scan the agent concluded that Kyllo was growing marijuana indoors. Based party on the results from the thermal imaging scan the agent was able to acquire a search warrant for the home which resulted in the finding of over 100 marijuana plants. Kyllo argued that the use of the thermal imager violated his Fourth Amendment rights.

In its opinion for *Kyllo* the court cited *Katz* as its guide to determine whether a search is a search under the sense of the Fourth Amendment or not. The Court claimed that "it would be foolish to content that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance in technology" (*Kyllo v. United States* 2001, 33-34). As support for this statement the Court cited aerial observation, where the contents and actions of a fenced in backyard may have been completely private in the past, the advent of the airplane makes it so that these locations can be monitored from above. The Court's concern though is to attempt to determine "what limits there are upon this power of technology to shrink the realm of guaranteed privacy" (*Kyllo v. United States* 2001, 34). The Court in this case noted that with respect to the interior of the home "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*" (*Kyllo v. United States* 2001, 34). To allow the use of technology to erode from the minimum protection granted within the home would then erode the guaranteed privacy granted by the Fourth Amendment. The court then held that

> obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman*, 365 U.S. at 512, constitutes a search – at least where (as here) the technology in question is not in general public use. (*Kyllo v. United States* 2001, 34).

Therefore the court found that the information obtained by the thermal imager was the product of a search. Given that this search was conducted without a warrant the findings were then invalid.

The Court also addressed the points made in the previous thermal imager cases that claimed that the imager merely measure heat outside the home. This type of argument was rejected by directly referencing *Katz* noting that in that case the eavesdropping device was invalidated even though it could have been said that it "picked up only sound waves that reached the exterior of the phone booth" (*Kyllo v. United States* 2001, 35). The court further argued that to allow such a claim to stand would run the risk of one day allowing some form of technology, for instance highly advanced thermal imagers, which could essentially grant complete knowledge of what went on inside a house. Ultimately though the Court in this instance did reference the Katz test it did not apply it given that it did not consider that its application was necessary when considering the actions Kyllo took within his home.

Common threads of reasoning that can be seen throughout the older cases examined above are that analogies are often utilized in order to ground these technologies to more understandable phenomena and make it easier to apply previous decisions to them. Furthermore when determining the legitimacy of an expectation of privacy in order

to determine whether a warrantless search was valid the courts deferred to the two pronged test outlined in *Katz* regardless of the technology used during the search. With respect to the internet then, to find that these trends continue would lend support to the notion that the internet is not an innovation so different that the courts' past tools no longer apply. With this in mind it is now time to examine cases where issues rise around the nexus between computers and the internet.

Internet-Related Cases

The case *United States v. Simons* (206 F.3d 392, 2000) is one of the earlier cases exemplifying the conflict that may occur between the Fourth Amendment and the internet. Mark Simons worked for the Foreign Bureau of Information Services (FBIS), a division of the CIA, and was provided a private office as well as a computer with internet access. The FBIS has a policy stating that internet use by employees was for official government business only. The policy explicitly forbade accessing unlawful material. Furthermore the policy warned that FBIS would ensure compliance with the policy by conducting electronic audits. When a manager was better familiarizing himself with a recently acquired firewall by entering the keyword "sex" he discovered that a large amount of hits originated from Simons' computer. It was readily evident from the websites' names that Simons had not been accessing them for work-related reasons.

A manager was contacted who then had a network administrator access Simons' computer to determine whether he had downloaded any of the pictures from the sites he had visited to his computer. The administrator printed the file names of the pictures as well as copied the files from Simons' hard drive. These tasks were all done remotely,

from the administrator's desk. Later the copied files were examined by members of the CIA Office of the Inspector General (OIG) who determined that some of the pictures were of minors. Then Simons' hard drive was removed from his computer and replaced with a copy and the original was given to an OIG criminal investigator. Based on the images from the hard drive a search warrant was attained for the files on Simons' computer as well as other materials in his office, such as diskettes and zip drives.

After being charged Simons tried to suppress the evidence gathered from the searches of his computer and office. Simons claimed the initial search of his computer by the firewall operator violated his Fourth Amendment rights since it had been performed without a warrant. The internet comes into play in two forms in this case. The first is as a tool Simons used to commit his crime, using it to attain child pornography. The second is as a tool used to search and gather evidence against Simons. It should be noted here that for the purposes of this work a computer network will be deemed analogous to access to the internet given that it grants many of the same properties, such as searching and communicating, but on a smaller scale.

The court in this case noted that "to establish a violation of his rights under the Fourth Amendment, Simons must first prove that he had a legitimate expectation of privacy in the place searched or the item seized" (*United States v. Simons* 2000, 398). To determine whether Simons presented a legitimate expectation of privacy the court relied on the Katz test. When trying to determine whether Simons demonstrated a legitimate objective expectation of privacy the court employed a line of reasoning that has been used in some cases above. This reasoning is that of creating an analogy between a novel form of technology to a more well-known and mundane phenomena. The *Simons* court

did this by pointing to *O'Connor v Ortega* in claiming that while "government employees may have a legitimate expectation of privacy in their offices or in parts of their offices such as their desks or file cabinets" it is also the case that "office practices, procedures, or regulations may reduce legitimate privacy expectations" (*United States v. Simons* 2000, 398).

The court felt that the reasoning given in *O'Connor* was applicable for Simons' situation because Simons' employer had a policy warning its employees that their internet use would be periodically monitored. Therefore, given that the court in *O'Connor* decided that having a comparable policy removed an employee's expectation of privacy, the court in this case found that "in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet" (*United States v. Simons* 2000, 398). Even if Simons may have subjectively thought his actions on the Internet remained private "such a belief was not objectively reasonable after [his employer] notified him that it would be overseeing his Internet use" (*United States v. Simons* 2000, 398). The Court likened Simons' usage of the internet after being warned that it would be subject to observation as him merely exposing his actions to a third party. The court concluded then that the search and seizure of Simons' computer and the files he downloaded from the internet did not violate the Fourth Amendment.

The case of *United States v. Hambrick* (U.S. App. LEXIS 18665, 2000) presented a situation much different than the kind found in *Simons*, indicating the potential variance of situations in which the Fourth Amendment may conflict with the internet. Scott Hambrick, a police captain, first contacted someone using the screen name Rory14 in an on-line chat-room called "#gaydads4sons." Hambrick believed that Rory14 was a

fourteen-year-old boy. Hambrick tried to start a sexual relationship with Rory14 and even sent $270 to a Post Office Box that Rory14 had given him. Along with the money Hambrick also sent detailed instructions with respect to meeting arrangements. Throughout all this correspondence Hambrick was unaware that Rory14 was actually Detective J.L. MacLaughlin, who was a member of a regional task force against internet crimes aimed at children.

After Hambrick and MacLaughlin, still under the guise of Rory14, chatted several times MacLaughlin sent Hambrick's Internet Service Provider (ISP) a subpoena asking for non-content information pertaining to Hambrick, who was only know to the detectives by his username at the time. The government later conceded during the trial that this subpoena was invalid given the faulty manner in which it was attained. The ISP complied with the subpoena and handed over Hambricks name, billing address, and IP address among other types of identifying information. After gathering this information MacLaughlin handed it, as well as control of the Rory14 account, over to the FBI. The FBI gathered more information from the ISP by using a "grand jury subpoena" which then helped them get a search warrant for Hambrick's residence. Hambrick argued the information gathered from his ISP had violated his Fourth Amendment rights given that it had been attained without using a valid warrant.

The court in this case once again cited *Katz* in its opinion noting that therein "the Supreme Court analyzed the scope of protection afforded by the Fourth Amendment, stating that a search occurs only when there has been a 'physical intrusion' in a 'constitutionally protected area,' noting further that the Fourth Amendment 'protects people not places'" (*United States v. Hambrick 2000*, 6). To determine whether the

Fourth Amendment protection applied the court once again referenced *Katz* and the test it delineated to determine whether Hambrick had a legitimate expectation of privacy. In actually applying the Katz test in this instance the court's reasoning relied heavily on *Smith*. As *Smith* found that some information given to the telephone company in the form of dialed numbers was not protected by the Fourth Amendment, the court in this case reasoned that "a person does not have an interest in the account information given to the ISP in order to establish [an] e-mail account" (*United States v. Hambrick* 2000, 12). Both the *Smith* and *Hambrick* courts considered the type of information that was given to the companies in these two cases was non-content information and therefore did not fall under Fourth Amendment protection. Furthermore the court re-iterated that "when an individual conveys information to a third party, the individual 'assumes the risk' of subsequent disclosure" (*United States v. Hambrick* 2000, 9). Therefore, since Hambrick voluntarily gave up certain, non-content, information to his service provider he had no legitimate expectation of privacy when it came to that information.

The case of *Guest v. Leis* (255 F.3d 325, 2001) involved another manner in which people socialize while online that was separate from the online chat rooms presented in *Hambrick*. The expectation of privacy that individuals have when posting in online bulletin boards was one issue in question in Guest v. Leis. The Hamilton County, Ohio, Regional Electronic Computer Intelligence Task Force (RECI) seized two computer bulletin board systems while in the process of investigating on-line obscenity. The systems seized were the Cincinnati Computer Connection Bulletin Board System (CCC BBS) and the Spanish Inquisition Bulletin Board System (SI BBS). Several users of each of the systems filed class action suits against RECI claiming they had violated the First

and Fourth Amendments among other violations. Though the agents in this case had valid warrants for the homes of those that hosted the bulletin boards, the users argued the search of the content they had transmitted to the boards had been done without a valid warrant once the host systems were seized.

In its opinion the court claimed that "in order to challenge a search or seizure as a violation of the Fourth Amendment, a person must have had a subjective expectation of privacy in the place or property to be searched which was objectively reasonable" (*Guest v. Leis* 2001, 333). This line of reasoning is of course consistent with that outlined in *Katz*. As was noted the case dealt with two bulletin board communities and the court affirmed that with respect to the users of the boards that they "would of course have a reasonable expectation of privacy in their homes and in their belongings—including computers—inside the home" (*Guest v. Leis* 2001, 333). Yet the court differentiated this expectation of privacy to the one the users have with respect to the servers on which the bulletin boards were hosted. Given that the users did not have any physical claim to the actual computers on which the boards' servers were hosted the court argued that they "would not share the same interest in someone else's house or computers, so they would not be able to challenge the search of the homes and the seizure of the computers as physical objects" (*Guest v. Leis* 2001, 333). The court went further and addressed the issue of the actual content that may be stored on seized computer that users may try to stake a privacy claim on.

With respect to one of the bulletin boards, the court dealt with the issue by pointing out that there was a disclaimer each user saw informing them that the messages they posted were not private. Therefore, as in *Simons*, the users could not claim an

objective privacy claim in the case. With respect to the second bulletin board, however, there was no such disclaimer. Once again the court found that there was no Fourth Amendment violation. The reasoning behind this was the same as that used in *United States v. King* wherein it was found that when someone sends content information through conventional mail, the sender loses their expectation of privacy with respect to that content upon delivery. Similarly in this case the court argued that "users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting" (*Guest v. Leis* 2001, 333). This is the case because the court considered posts to the bulletin board to be similar to emails available for the public to see so "they would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient" (*Guest v. Leis* 2001, 333). Therefore the content any users may have posted on the bulletin board could not be said to be objectively private. Given these findings the court ruled that there were no Fourth Amendment violations.

In *United States v. Angevine* (281 F.3d 1130, 2002) a situation similar to that of *Simons* was presented. Eric Angevine was a professor of Architecture at Oklahoma State University. The University provided him with an office computer connected to both the University network as well as the internet. Angevine used the computer to download thousands of pornographic images of young boys, printed them, then deleted the images from his computer. Using the help of Angevine's wife the police were able to obtain a search warrant for his University computer. After seizing the computer the police were able to retrieve pornographic files that had remained in the memory despite Angevine's attempts of deletion. Angevine argued that the warrant the police obtained was invalid because the police had recklessly omitted important information in the affidavit they used

to obtain the warrant. Simlarly as in *Meriwether* described above, even though the warrant in this case was found to be valid the court specifically addresses the question of whether this search would have been valid under the Fourth Amendment even if there had been no warrant.

The court argued that in order to establish a Fourth Amendment violation Angevine must have demonstrated a legitimate expectation of privacy in the place search or the item seized. The existence of this expectation in turn was determined by the application of the test outlined in *Katz*. Once again in this case the court pointed to the policy that Angevine's employer, the Oklahoma State University, had in place with respect to internet use. The university's policy included warnings that they "reserved the right to randomly audit Internet use" as well as any information flowing through the network would not be "confidential either in transit or storage" (*United States v. Angevine* 2002, 1134). The court in this case concluded that "Oklahoma State University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers" given that it warned the user of the potential for monitoring the Internet use of individuals (*United States v. Angevine* 2002, 1134). Therefore the court found that Angevine's Fourth Amendment rights were not violated since he did not present a legitimate expectation of privacy.

Another case involving one's expectation of privacy while using the internet in the workplace is *United States v. Slanina* (283 F.3d 670, 2002). Wesley Slanina was a Fire Marshall for Webster, Texas whose desk was in City Hall. His city-provided computer had internet access but was not connected to the office network. After a new fire station was built Slanina was given his own office in the new building. He moved his

old computer into the new office wherein he had no internet access or network connection. Later on Ryan Smith, the Management Information Systems Coordinator, began work on installing the city's network onto the computers in the new fire station. Slanina was not at work the day Smith was going to install the network on his computer. When Smith attempted to do so he found that even though the computer was on it had a password-protected screensaver. Smith attempted to bypass this problem by restarting the computer only to discover that Slanina also had a BIOS password. Without this password Smith would be unable to access the computer's hard drive and would therefore be unable to install the network on his computer.

Smith called Slanina's supervisor who in turn called Slanina to obtain the password. The supervisor informed Slanina of the situation and told him to give Smith the password. Slanina was reluctant to give him his password and wanted to know exactly what Smith planned to do on the computer. To Smith's surprise roughly 10 minutes after getting the password Slanina showed up at the office asking how much longer the installation would take. Smith was suspicious by this point and told Slanina it would take hours when he knew it would take less. Slanina stayed for a while and would hop on his computer whenever Smith left the room. After Slanina left Smith noticed that he had left his email running while minimized. As Smith attempted to close it he noticed that Slanina had subscribed to newsgroups. Smith had been told that employees were barred from accessing newsgroups from work, but not all employees had been informed of this policy, including Slanina. Smith expanded the email to examine the newsgroups Slanina frequented. He noticed some of them were pornographic in nature with one's name implying it featured child pornography. Smith contact several supervisors and the

next day, with Slanina still out of the office, they examined his computer more closely including his zip drive and found child pornography on it. Ultimately all the evidence was handed over to the FBI. Slanina questioned the validity of this search given that it was performed without a warrant.

The court's decision with respect to Slanina's expectation of privacy differs in this case when compared to the previously examined cases. The court looked into Slanina's expectation of privacy in order to determine whether his claim that his Fourth Amendment rights were violated had any merit. With respect to a subjective expectation of privacy the court accepted that Slanina did express this, noting that his computer was in his office, his door was closed and locked, and furthermore his office computer was protected against third parties by having a password on it. Furthermore even though Slanina willingly gave his password to a third party the court found that he still rightly had a subjective expectation of privacy given that the password was given for a very limited purpose.

With respect to the second prong of the test, determining whether his expectation of privacy was objectively reasonable, the court once again sided with Slanina. Part of the reasoning behind this was that "even though network administrators and computer technicians necessarily had some access to his computer, there [was] no evidence that such access was routine" (*United States v. Slanina* 2002, 676). Furthermore the court found that in this case, as opposed to in *Simons*, there was no dissemination of "any policy that prevented the storage of personal information on city computers" by the city, Slanina's employer, and also it "did not inform its employees that computer usage and internet access would be monitored" (*United States v. Slanina* 2002, 676). Therefore

"given the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer" the court found that the objective prong of the *Katz* test was also satisfied (*United States v. Slanina* 2002, 677).

However, even though the court found that Slanina had a reasonable expectation of privacy in both his office and computer the court still upheld the warrantless search. The reasoning behind this decision relied heavily on *O'Connor v. Ortega* (480 U.S. 709, 1987). *O'Connor* presented a somewhat comparable real-world counterpart to Slanina's situation given that it dealt with a doctor's desk and file cabinets that were search by a state hospital administrator without a warrant. Though the Court found in that case that the doctor held a reasonable expectation of privacy they still upheld the warrantless search noting that "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all circumstances" (*O'Connor v. Ortega* 1987, 725-726). The court in this case then ultimately agreed with the *O'Connor* Court and upheld the warrantless search.

The case of *United States v. Lifshitz* (369 F.3d 173, 2004) is a relatively unique case given that it involves and individual on probation, which presents new considerations for the court. After the FBI had conducted an investigation in which they found that Brandon Lifshitz had been downloading child pornography as well as disseminating it by posting it on websites Lifshitz pled guilty pursuant to a plea bargain he had made. Part of Lifshitz's deal included a lesser punishment because he had argued

he was suffering from a reduced mental capacity at the time of his offense. The court, taking the opinions of four doctors into consideration, ended up sentencing Lifshitz to three years' probation.

One of Lifshitz's conditions of probation was that he would allow his computer to be monitored on a regular or random basis. He would also have to allow the copying of all the data from his computer and any peripherals for the purpose of conducting a more thorough examination. This was the condition that Lifshitz's defense objected to given that this would amount to Lifshitz being subject to many unwarranted searches, violating his Fourth Amendment rights.

As has been noted in many of the cases examined above, including those involving older technological innovations, analogies are often used in order to make a novel situation more manageable. In this the court questioned the potential problem that may arise when using analogies with respect to computers. The problem with trying to compare computer monitoring with other actions arises given that

> ultimately, the attempt to establish the best point of comparison with all computer monitoring may prove futile, because computers serve a multiplicity of functions, from mailbox (in sending and receiving e-mail), to telephone (in accessing particular IP addresses and web pages), to financial systems (by both permitting on-line payment mechanism and recording personal financial data), to home offices, to storage bins. (*United States v. Lifshitz* 2004, 183)

A blanket comparison about computer monitoring, then, cannot always be applied between computers and real-world actions. Despite this word of caution, however, the

court noted that "the available analogies do, however, provide some assistance in assessing the nature and scope of a potential intrusion into computer privacy" (United *States v. Lifshitz* 2004, 183). In this particular case, then, the Court considered the analogy between drug testing and the type of computer monitoring in question.

When addressing the issue at hand the *Lifshitz* court acknowledged, citing *Guest*, that while individuals generally possess a reasonable expectation of privacy in their home computers, they may not enjoy such an expectation of privacy in transmissions over the internet or email that have already arrived at the recipient. The way in which this case differed from other similar cases, however, is that Lifshitz, being on probation, was judged against the "special needs" of probationary searches. The court identified the "special needs" standard as it was described in *Griffin v. Wisconsin* (483 U.S. 868, 1987) and expanded upon in *United States v. Knights* (534 U.S. 112, 2001). The court took the rulings in these cases to amount to mean that "in the case of a probationer, the imposition of a search condition as part of probation creates a diminished expectation of privacy" (*United States v. Lifshitz* 2004, 180).

The court then proceeded by nothing that "the context in which the doctrine of 'special needs' has been most thoroughly developed is that of drug testing" (*United States v. Lifshitz* 2004, 183). The court, therefore, attempted to compare the computer monitoring in question to drug testing, noting that "regular searches of a probationer's computer, on the one hand, and of his urine or sweat, on the other, can deter him from engaging in impermissible conduct" (United States v. Lifshitz 2004, 189). It concluded then that the "special needs" of the probation system justified the requirement of Lifshitz's computer monitoring but remanded the case cautioning that the scope of the

monitoring may have been too broad. The court elaborated on this point by noting that that drug testing is aimed at only determining whether or not an individual has used illegal substances and any other type of information gathered from that testing is inconsequential.

In *United States v. Heckenkamp* (482 F.3d 1142. 2007) the court once again addressed the issue of a "special needs" case. After Scott Kennedy noticed that someone had hacked into his company's, Qualcomm Corporation, computer network he traced the intrusion to a computer on the University of Wisconsin at Madison's network. Kennedy contacted Jeffrey Savoy, the university's network investigator, who then began to examine the network for any problems. Savoy confirmed that someone from the university's network had indeed tried to hack into Qualcomm's system as well as the university's email server. Fearing a massive disruption on campus due to this intrusion, Savoy investigated further and managed to trace the intrusion to a computer in one of the university's dormitories. Savoy determined that the person who had performed the intrusion was Jerome Heckenkamp, who he knew had previously worked for the university's computer help desk before being fired. Savoy also knew that Heckenkamp had the technical knowledge that could be used to damage the university's system.

Savoy contacted FBI agent Terry Rankhorn and informed him about what he had found. Rankhorn told Savoy he intended to get a warrant for the computer but he did not tell Savoy to investigate further. Savoy was still concerned about the university system's integrity and continued to monitor the computer's activity. Based on what he observed Savoy felt that he needed to get the machine offline as soon as possible. Together with the university police Savoy went to Heckenkamp's room and after he voluntarily gave

them his password it was verified that he was the one who hacked the systems. All of this took place before the FBI had actually attained a search warrant even though they were not directly involved. Heckenkamp argued for suppressing the evidence gathered from Savoy monitoring his computer given that he did not have a search warrant.

This case is somewhat unique because the court noted in its opinion that "the government [did] not dispute that Heckenkamp had a subjective expectation of privacy in his computer and his dormitory room, and there is no doubt that Heckenkamp's subjective expectation as to the latter was legitimate and objectively reasonable" (*United States v. Heckenkcamp* 2007, 1146). Furthermore, citing *Lifshitz*, the Court also recognized that Heckencamp had a "legitimate, objectively reasonable expectation of privacy in his personal computer" (*United States v. Heckenkcamp* 2007, 1146). Given these two findings, then, a warrantless search would usually not be considered valid under the Fourth Amendment. Yet this case had the complicating factor that the computer was connected to a network. Ultimately the court found that under the facts of this particular case that "the act of attaching his computer to the network did not extinguish his legitimate, objectively reasonable privacy expectation" (*United States v. Heckenkcamp* 2007, 1146). Yet the court cited *Angevine* when noting that "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that systems administrators may monitor communications transmitted by the user" (United States v. Heckenkcamp 2007, 1147). In this particular case, however, no such warning was given, leading the court to determine that Heckenkamp's expectation of privacy remained intact, unlike in *Angevine* and *Simons*.

Even though there was no question as to the legitimacy of the claim of an expectation of privacy in *Heckenkamp* as outlined above, the court nevertheless found the warrantless search at issue to be justified. The court found in this case that "the search of the computer was justified under the 'special needs' exception to the warrant requirement" (*United States v. Heckenkcamp* 2007, 1147). Whereas the 'special needs' in *Lifshitz* dealt with the search of a parolee, in this case it dealt with a network administrator, Savoy, searching Heckenkamp's computer in order safeguard the integrity and security of the network to which it was connected. The court claimed that "requiring a warrant to investigate potential misuse of the university's computer network would disrupt the operation of the university and the network that it relies upon in order to function" (*United States v. Heckenkcamp* 2007, 1148). Combined with the fact that "Savoy was acting purely within the scope of his role as a system administrator" acting to "rectify an emergency" the court found that the "special needs" exception was justified (*United States v. Heckenkcamp* 2007, 1147). The warrantless remote search of his computer was then considered valid by the court. This case and the previous case reveal some flexibility when applying the Fourth Amendment to the internet given that under some circumstances a "special needs" standard may be employed.

In *United States v. King* (509 F.3d 1338, 2007) one of the more fundamental file sharing systems scrutinized by the court. While Michael King was working as a civilian contractor in Saudi Arabia he lived in a dormitory at the Prince Sultan Air Base. He kept his personal laptop in his room, connected to the base's network. He was aware that his activities while connected to the network were subject to monitoring. King thought that he had properly secured his computer so that others were unable to access it. One day an

enlisted airman was browsing through the base's network, searching for music files, when he ran across King's computer. Given that King's hard drive was a "shared" drive the airman was freely able to access it and look at its contents. Along with music files the airman also found a pornographic movie as well as pornographic text files on the hard drive.

The airman reported his findings to a military investigator who then contacted a computer specialist. The specialist located and accessed King's computer on the network, using the same means as the airman, and confirmed the airman's findings and also found an empty folder on the hard drive labeled "pedophilia." The specialist then reported her findings to the investigator, who proceeded to obtain a search warrant for king's room. The search of King's room yielded cd's and hard drives containing thousands of images of child pornography. King argued that the search of his computer violated his Fourth Amendment rights because it had been conducted without a warrant.

The court in this case once again noted that the Fourth Amendment protects individuals from unreasonable searches and seizures in those places where they can demonstrate a reasonable expectation of privacy. This is done as was described in *Katz* by demonstrating both an objective and subjective expectation of privacy. With respect to a subjective expectation of privacy the court found that given King's "experience with computer security and the affirmative steps he took to install security setting" that he adequately demonstrated his subjective expectation of privacy (*United States v. King* 2007, 1341). With respect to the second prong of the test the court found that given that King's laptop was connected to a military base network then his "files were 'shared' over the entire base network, and that everyone on the network had access to all his files and

could observe them in exactly the same manner as the computer specialist did" (*United States v. King* 2007, 1342). Therefore "the content of his computer's hard drive were akin to items stored in the unsecured common areas of a multi-unit apartment building or put in a dumpster accessible to the public" (United States v. King 2007, 1342). Given that the items in this analogy were previously found not to be worthy of an objective expectation of privacy, the court concluded that in this case King also did not hold an objective expectation of privacy to the files he had shared through the network. King's claim that his Fourth Amendment rights were violated was found by the court to be without merit.

Yet another workplace example of the Fourth Amendment conflicting with the internet is presented in *United States v. Barrows* (481 F.3d 1246, 2007). Rather than involving a work-issued computer, however, it involves one brought from the defendant's home. Michael Barrows worked as the treasurer of Glencoe, Oklahoma. He did not have a private office and instead shared his workspace with the city clerk. This workspace was located in an open area of city hall although it was separated from the general public by a counter. Barrows and the clerk had little privacy in their workspace given that other employees frequently entered the space to use the fax machine and copier located about a foot from their desk. The two also shared a computer which they used to access city records. Barrows brought his personal computer from home and placed it on their desk. He connected the computer to the city's network and told his co-worker that they could now input and access information simultaneously from either computer.

Barrows did not attempt to protect the files on his computer by placing a password on it. Furthermore he even left the computer on all the time, even when he was away from the desk. Around the time Barrows had connected his computer to the

network the clerk started to have problems when trying to access files using the city machine. She informed Michael McQuown, a reserve police officer who happened to be near the desk at the time, about the problem given that he had helped her with computer problems in the past.

McQuown attempted to fix the problem for a while and after the clerk informed him that Barrows had networked the computer he suspected that the problem they had with opening a file may have been due to the file being open on Barrows' computer. Barrows was not at the desk at the time but the computer was on as usual so McQuown used it to try to solve the problem. McQuown quickly noticed that the computer was running a file-sharing program so he opened it and looked at the transfer history to determine if he had transferred the file they were trying to access. In the transfer history he found many files with sexually suggestive names that were revealed to be child pornography after he opened a few of them. Afterward McQuown and the sheriff seized Barrows' computer and obtained a search warrant in order to search the hard drive. Barrows argued for the suppression of all the information gathered from his computer claiming that the search had violated his Fourth Amendment rights given that the first search had been done without a warrant.

The court once again made clear that a warrantless search may be unreasonable if it occurs even though the defendant held a legitimate expectation of privacy. This determination was made by applying the two pronged test outlined in *Katz.* The expectation of privacy was found to be invalid both subjective and objectively. Unlike in *Slanina,* Barrows did not protect his computer with a password, turn it off, or do anything else in order to stop a third party from using it. Furthermore the court noted that he was

working in a public area where "the chances a passerby might spy snatches of personal material over his shoulder, or sit down to use his computer having honestly mistaken it for a city one, were appreciable" (*United States v. Barrows* 2007, 1249). Taking these facts into account the court claimed it was "hard-pressed to conclude that Mr. Barrows harbored a subjective expectation of privacy" (*United States v. Barrows* 2007, 1249). Barrows further claimed that he did not invite anyone else to use his access his computer, yet similarly as in *King*, the court found that "he knowingly networked his machine to the city computer for the express purpose of sharing files" (*United States v. Barrows* 2007, 1249). Given that Barrows made no reasonable attempts at blocking his personal information from being viewed from third parties the court found he held no objective expectation of privacy either. Having failed both portions of the *Katz* test the court found that Barrows did not hold a legitimate expectation of privacy so the warrantless search did not violate his Fourth Amendment rights.

In *United States v. Perrine* (518 F.3d 1196, 2008) involves internet chat rooms, peer-to-peer file sharing software, and also hints at the distinction between content and non-content information that will be expanded upon later. James Vanlandingham from Pennsylvania was in a Yahoo! Chat room when he began chatting with a person whose screen name was "stevedragonslayer." This user invited Vanlandingham to watch a web cam video that featured two nude girls. Vanlandingham contacted the local police after he had been shown the video but continued the chat with stevedragonslayer. Before the police arrived at Vanlandingham's house stevedragonslayer showed him more videos depicting you girls performing explicit sexual acts. The chat had ceased by the time police arrived but Vanlandingham had saved the chat conversation.

Based on Valaningham's information the police obtained the subscriber information for the chat user stevedragonslayer from Yahoo! who was able to provide them with his IP address. After they got the IP the police identified that it was maintained by Cox Communications, Inc. The police sought the subscriber information for the person tied to the IP from Cox and were given information regarding stevendragonslayer's true identity. The user stevedragonslayer was actually Steve Perrine from Wichita, Kansas. The Pennsylvania police contacted the Kansas authorities who were able to obtain a search warrant for Perrine's house. The police found thousands of child pornography images on Perrine's computer and also noted that Perrine had installed Kazaa, a peer-to-peer file sharing program, on his computer. One of Perrine's arguments was that his Fourth Amendment rights were violated when the police obtained his subscriber information from Yahoo! and Cox.

In this case the court pointed to several other cases such as *Hambrick*, *Guest*, and *Lifshitz* among other lower court decisions to support its finding that the information one gives to an internet service provider cannot be said to be protected by the Fourth Amendment. The court also noted that Perrine installed peer-to-peer software on his computer "which permitted anyone else on the internet to access at least certain folders in his computer" and concluded that this action "additionally vitiates any expectations of privacy he might have [had] in his computer and its content" (*United States v. Perrine* 2008, 1205). The court concluded therefore that Perrine had no privacy expectation with neither his subscriber information nor with the content on his computer.

The case of *United States v. Forrester* (512 F.3d 500, 2008) is perhaps the one examined here that most closely resembles one of the pre-internet cases so the manner in

which the court treated it may prove to be particularly interesting. Mark Forrester and Dennis Alba were being investigated over a suspected Ecstasy manufacturing operation. During its investigation the government used a "mirror port" to monitor Alba's email and internet activity. The mirror port is analogous to a pen register and kept track of the to/from addresses of any emails sent, the IP addresses of websites visited, as well as the amount of information sent or received by the account. The use of this device was challenged by Alba given that it monitored his activity without the need of a warrant.

As it may have been expected in this case's reasoning the court drew upon the reasoning used in *Smith v. Maryland* greatly given that it considered the questions at issue to be quite analogous. The court first reasoned that "e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication" (*United States v. Forrester* 2008, 510). Where telephone users require intervention from the phone company to communicate, internet users require an internet service provider to communicate. So, similarly to *Smith*, the court claimed that

> E-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing information. (*United States v. Forrester* 2008, 510)

The court further reasoned that "the government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail" (*United States v. Forrester* 2008, 511). Since the case only involved the government obtaining the "the to/from addresses of a person's

e-mails or the IP addresses of websites visited" and did not gather anything regarding the content of these addresses, the information gathered was no more intrusive than examining the outside of a piece of mail (*United States v. Forrester* 2008, 510). The court argued that while they knew the IP addresses of the websites visited they could not tell which particular pages on that website were viewed. The court once again compared this observation to a less technologically advanced one noting that "like IP addresses, certain phone numbers may strongly indicate the underlying content of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms" (*United States v. Forrester* 2008, 510). Therefore in this instance, as in *Smith*, there was no Fourth Amendment violation since the court found in this case that the use of the mirror port did not constitute a search under the Fourth Amendment.

While the use of a peer-to-peer program to share files was mentioned in passing in *Perrine*, such a program played a larger role in *United States v. Ganoe* (538 F.3d 1117, 2008). Special Agent for Immigration and Customs Enforcement Ken Rochford was trying to locate people trading child pornography online via the peer-to-peer file sharing program LimeWire. Rochford found a video he suspected of being child pornography which he confirmed after downloading and viewing it. Through LimeWire Rochford was able the view rest of the files being shared by the person that hosted the video. His inspection revealed more files containing similar content. Rochford was able to determine the host computer's IP address and that led to him finding out that the IP address belonged to Tyrone Ganoe. Rochford also obtained Ganoe's physical address as well as a

search warrant for his house. Ganoe argued the initial search of his computer without a warrant violated his Fourth Amendment rights.

The court reiterated that a person generally has an objectively reasonable expectation of privacy with respect to their personal computer but this expectation is altered when one installs file sharing software on their computer. The court found that the claim of an expectation of privacy cannot survive the "decision to install and use file-sharing software, thereby opening [one's] computer to anyone else with the same freely available program" (*United States v. Ganoe* 2008, 1127). Even though Ganoe claimed he did not know others would be able to remotely access the files stored on his computer when installing the software the court rebutted that claim by pointing out that "he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network" (*United States v. Ganoe* 2008, 1127). Taking these facts into account the court found that Ganoe could not adequately demonstrate an expectation of privacy that society would consider reasonable so he could therefore not invoke Fourth Amendment protection.

The case of *United States v. Stults* (575 F.3d 834, 2009) also focused on the issue of file-sharing. FBI agent Joseph Cecchini used LimeWire to search for potential hosts of child pornography. He encountered one user with various files depicting child pornography. Cecchini obtained the IP address of the user using LimeWire and then attained a subpoena to get the ISP, Cox Communications, to hand over the subscriber information based on the IP address. The user hosting the child pornography was identified as Harold Stults. A warrant was obtained for Stults' house that when executed yielded more instances of child pornography on Stults' computer. Stults argued that the

warrant was obtained based on evidence gathered from an illegal search of his computer through peer-to-peer file sharing software.

Once again the court wished to determine whether Stults held a legitimate expectation of privacy with may have invalidated the warrantless search conducted on his computer. The key question to determine this as phrased by the court was then "whether Stults had both a subjective and objectively reasonable expectation of privacy in files accessed through Stults's installation and use of LimeWire, P2P file-sharing software" (*United States v. Stults* 2009, 842). The court cited cases such as *Ganoe*, *Perrine*, and *Barrows* to solidify the point that when one allows access to the content of their computer either via the installation of file-sharing programs, as in *Ganoe* and *Perrine*, or through connecting to a network, as in *Barrows*, while they may have had a legitimate expectation of privacy before, that expectation is removed. The installation of the file-sharing software therefore removed any objective expectation of privacy Stults may have had otherwise. Therefore Stults was not found to have met the requirement to invoke Fourth Amendment protection.

One of the most recent internet related Fourth Amendment cases that has also received a fair amount of attention is *United States v. Warshak* (631 F.3d 266, 2010). Steven Warshak was the owner of a business that came under the scrutiny of the Better Business Bureau. Many customers had complained about the company's auto-ship program that would continue to charge and send them products unless they opted out, though they had never been told they had to. Warshak had also been under investigation for other reasons. Warshak's company relied heavily on email communication between its employees. One of his email accounts was provided by the ISP NuVox

Communications. During their investigation the government requested that NuVox preserve the contents of any emails Warshak sent or received. Warshak was not informed that his emails were being preserved. The government did not review the emails until later when it had obtained a subpoena to do so. Warshak was also not aware of this subpoena. Warshak argued that the seizure of these roughly 27,000 emails violated his Fourth Amendment rights given many of the emails were gathered before a warrant was obtained.

As is made evident by the outlines of the cases chosen above, the types of situations in which the Fourth Amendment comes into conflict with the internet are manifested in many ways. The diversity between these cases is beneficial for the purposes of this work because it can speak to the efficacy of past principles if they are found to be applied consistently in these varying scenarios. Furthermore when looking at both the internet related cases and those involving past technologies it is evident that while most of the cases are incomparable in terms of the types of actions that took place there are also some that can be seen as analogous, such as *Smith* and *Forrester*. Once again this variance can potentially highlight any differences or similarities used between the reasoning in the cases.

The court once again applied the subjective and objective expectation of privacy test when considering whether Warshak had a valid Fourth Amendment claim in this instance. The reason this case was more high profile than other internet related cases is because it involved the access to the content of emails rather than just their non-content information. With respect to the subjective portion of the test the court found that "Warshak plainly manifested an expectation that his email would be shielded from

outside scrutiny" (*United States v. Warshak* 2010, 284). They based this on the substantive information contained in the emails, highly doubting that it was the kind of information someone would want to present to the public.

As a preface to addressing the objective expectation of privacy with respect to email content the court made explicit the fact that email has become a very common tool individuals use in today's society and that through email people transmit countless amounts of sensitive information. Given this high degree of importance email has achieved in many people's lives the court stated that much hinges "on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment" (*United States v. Warshak* 2010, 284). The court compared email to telephone conversations as well as conventional mail, citing *Katz* as well as *Ex Parte Jackson,* to make the point that the content of the types of communication these cases address cannot be examined without police first obtaining a warrant after demonstrating probable cause. Therefore the court concluded that "given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford email lesser Fourth Amendment protection" (*United States v. Warshak* 2010, 285-286). Given that the court considered email to be analogous to a phone call or a letter it then compared the ISP to a post office or telephone company. It follows from this reasoning that the police would not be able to compel an ISP from handing over the content information from emails since "the police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant, that is" (*United States v. Warshak* 2010, 286).

The court also took into consideration the subscription agreement that Warshak had agreed to when signing up with his ISP that stated that it "*may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service'" (*United States v. Warshak* 2010, 287). Yet the court was "convinced that some degree of routine access is hardly dispositive with respect to the privacy question" (*United States v. Warshak* 2010, 287). It did recognize that there may be some agreements, however, where if an ISP warns of frequent monitoring of emails then that would make an expectation of privacy unreasonable. Taking all these factors into account the court decided that in cases such as the one presented "the government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause" (*United States v. Warshak* 2010, 288). The court then concluded that government agents violated the Fourth Amendment when they obtained the contents of Warshak's emails without a warrant. The court went even further in this case and addressed the Stored Communications Act (SCA) which is a "statute that allows the government to obtain certain electronic communications without procuring a warrant" (*United States v. Warshak* 2010, 282). The court found that this portion of the statute, for the reasons noted above, to be unconstitutional.

There are a few trends that one can gather from examining the reasoning behind the cases highlighted above. Perhaps the most obvious common reasoning tactic used throughout these cases was the application of the reasonable expectation of privacy test. The pervasiveness of this test is evident given that it was used in all cases, even those concerning widely different types of technological innovations. With respect to the question at issue here the constant application of this approach can lend some insight as

to the relationship between the law and the internet. At the very least what this has demonstrated is that the internet may not be an innovation so new and revolutionary that previously established principles are not well-suited enough to deal with the legal problems that arise in it.

A second trend that is observed from examining the cases above is the willingness of courts to apply analogies when faced with novel technologies. When faced with a situation that may not have been directly addressed before courts looked for analogues of the situation in more familiar contexts. Thermal imagers were likened to drug sniffing dogs, email was compared to conventional mail, files stored in a shared folder were seen as analogous to items placed in a communal area, and more.

The perseverance of the third party doctrine can also be seen throughout the cases examined above. From *Smith* in 1979 to *Warshak* in 2010 and in many cases in between the courts frequently considered whether information that one transmits is likely to wind up in the hands of a third party and if it does then one's expectation of privacy with respect to that information or at least some aspect of it may fall.

There is also evidence of flexibility in the way in which the courts approach Fourth Amendment issues with respect to the internet. The cases of *Heckenkamp* and *Lifshitz* for instance demonstrate that courts can utilize exceptions, such as the "special needs" exception, in order to more adequately respond to particular issues raised by certain cases. Even in these cases, however, the use of the "special needs" exception was grounded in more familiar situations via the use of analogies.

One particular trend that is seen only in the internet-related cases above is the idea of one's expectation of privacy while online being diminished, even in one's home, by

some kind of disclaimer. For instance, in work environments company policies were considered enough to make warrantless searches valid. This finding may not seem very surprising in the context of the workplace but what may be more surprising, however, is that when at home one's expectation of privacy may be eroded as well. For example by installing some particular software, as the peer-to-peer file sharing cases demonstrated, or due to some contract with one's ISP, as the court in *Warshak* implied others may then be able to examine the content of your computer.

One trend that is also significant for the purpose of this work is the noted absence of innovation. This does not refer to technological innovation, which was obviously not lacking, but rather an absence in innovation in reasoning when addressing these issues. It should be noted that this case study was quite narrow in the much larger realm of conflict between the law and the internet, but nevertheless throughout the decades that the survey spanned courts did not have to create wholly new principles or techniques in order to deal with the issues when it came to the conflicts involving the internet and the Fourth Amendment.

Ultimately then, insofar as the small scope taken here can speak to, these cases have demonstrated that the internet is not necessarily the paradigm shattering innovation that some may fear it is. It is not an entity unable to be regulated, a veritable "no man's land," on the contrary as these cases have demonstrated, decades old techniques are still readily amenable to this new frontier, at least to an extent.

Chapter 4: Discussion and Conclusion

Having presented the findings after analyzing several cases involving technology and the internet the question of how the law, at least with respect to the Fourth Amendment, and the internet interact can now be addressed. As the problem was initially framed in the context of the debate between those who feel the internet can be readily regulated against those who do not it makes sense to frame the findings and conclusions within this context as well. After discussing the findings in this manner it is apt to critically reflect on the actual approach that was taken. Tied closely to this retrospective view of the process is a consideration of the applicability and generalizability of the results.

It is fairly evident that with respect to the debate concerning the "regulability," as Lessig (1999) describes it, of cyberspace that the internet is indeed capable of being regulated at least to a degree. The internet has undoubtedly become intertwined with many aspects of everyday life for most individuals yet the fear that some may have had of cyperspace being a sort of "no man's land" with respect to the law is overblown. Looking at the manner in which courts apply the laws should have indicated that this perhaps never was going to be the case.

The courts' reactions to previous technological innovations demonstrates that through analogies and consistent application of legal principles they are able to ground their reasoning when dealing with new technologies to past, better understood and more concretely grounded with respect to the law, phenomena. The cases examined here displayed time and again that the *Katz* rationale persists throughout wildly varying technological changes. Skeptics should have foreseen that this approach is applicable

with respect to the internet even though it may have created tenuous bonds at best in their eyes. What further emphasizes the robust nature of the *Katz* reasoning is that even when looking at the internet alone, which was shown to present many potential scenarios pertaining to the application of the Fourth Amendment, it was nevertheless applied consistently. There are others, however, that accept that the law and the internet can function together yet question the efficacy of this relationship. The concerns of these scholars could raise doubts with respect to the continued application of the *Katz* rationale. Simply because it has been applied consistently so far does not imply that this will continue to be the case.

The opposite end of the debate about the internet's regulability is harder to determine. Within this school of thought are those who think that the internet does not pose an impediment when it comes to applying the law. As the findings here demonstrate this point of view appears to more accurately represent how the law, with respect to the Fourth Amendment, and the internet actually interact. The third party principle, the *Katz* test, special needs exceptions, and other principles are all found to be readily applied to cases involving the internet. As was mentioned above, what is more debatable, however, is the underlying effectiveness of applying the law to the internet. This is the debate that has implications on whether the *Katz* rationale can continue to endure. If the *Katz* reasoning continues to be applied in the face of even newer innovations yet it cannot be said to serve the same fundamental purpose this may perhaps indicate the need to find a new approach. Fortunately as the cases here have demonstrated, however, this is not yet the case.

It is one thing to be able to apply old principles online but it is another for these principles to have the same effect online as they do in the physical world. For instance is the expectation of privacy one has online as readily discernable as in the physical world? The internet is still a relatively new innovation meaning that many individuals may still be ignorant when it comes to what repercussions their actions may have online. The implications of the answer to this question are further compounded by the pace of technological growth, which is increasingly uniting the online and offline worlds. So can the law possibly adapt at the rate necessary to stay relevant alongside the rapidly changing cyberworld? This secondary debate will be addressed shortly.

Looking at the cases examined as a whole it is evident that insofar as the *Katz* test was applied it was done so consistently throughout, with the exception of *Kyllo v. United States*. Yet *Kyllo* was important to consider given that its ruling went contrary to cases such as *United States v. Pinson* and *United States v. Ford*, both of which dealt with the same technological innovation and actually employed the *Katz* rationale. The *Kyllo* Court ultimately, however, did not arrive at its differing outcome due to a different application or replacement of the *Katz* reasoning. Rather it did so by placing a large premium on the privacy one has in their home while simultaneously attempting to curb the ability certain technologies may have in shrinking the sphere of privacy.

One may ask how an intrusion into the privacy of the home can be invalidated in *Kyllo* yet it was not found to be a problem in cases such as *United States v. Ganoe* or *United States v. Stults.* In each of these cases warrantless searches were conducted on the defendants, more specifically on their personal computers located within their own homes, yet the searches were found to not have violated their Fourth Amendment rights.

The *Kyllo* Court appeared to warn about this kind of intrusion. In actuality, however, the *Kyllo* Court forbade such searches when they involved the use of technology by the government that was not in general public use. Obviously then, both the internet as well as the file sharing software that opened these monitoring avenues in the first place against the defendants in *Ganoe* and *Stults* were both in general public use. Therefore though *Kyllo* may at first blush be seen as an outlier in the sample set not only does its reasoning not conflict with the later cases but it may assuage the doubts of those that wonder why the home is not as impregnable as one would expect when it comes to the internet.

Overall, *Kyllo* aside, it is fairly evident that the cases examined here were treated consistently; there were no obvious instances of encountering a situation so novel that a new principle was needed. On the contrary some cases could even be seen to parallel each other between the physical and cyber worlds. *Smith v. Maryland* for instance is very similar to *United States v. Forrester* and the situation in *United States v. Katz* could be seen as comparable to that of *United States v. Warshak* at least when examining the issues that are functionally at stake. The ability to apply the *Katz* rationale in such functionally different scenarios also supports its continued application in the face of even newer technologies given that they may be ultimately rooted in more manageable terms. Yet taking these findings and claiming that one can conclude that the internet is truly nothing new would be a simplistic claim. It is indeed evident that old laws can be applied to the internet in an apparently easy manner but as many scholars have noted the more pertinent question may be whether doing so is truly effective and the optimum solution for handling the law on the internet. As was noted earlier in this work, Kerr (2010)

addressed both these issues and asked whether the previously established legal rules still fulfill their intended function in the new technological realm.

In order to stay true to the spirit of the old laws, Kerr posits that an overt link should be made between the physical and online worlds that more clearly informs courts with how to handle certain issues that arise online. The findings presented here may question the necessity of explicitly adopting the kind of connections that Kerr proposes such as equating certain kinds of physical surveillance to the monitoring of content and non-content information online. As *United States v. Warshak, United States v. Hambrick,* and *Guest v. Leis* have demonstrated courts have already taken into account the distinction between content and non-content information online without the need of external guidelines informing them on how to do so. Yet this does not necessarily mean that Kerr's claims are wholly without merit. On the contrary, such an overt distinction between the types of content may become more import as technology advances, as will be discussed later.

Another issue some scholars such as Tyson (2010) and Grubins (2008) point out with regards to the efficacy of the courts in dealing with the problems that may be raised with respect to the law and the internet revolves around which approach should be taken to address these issues: a judicial one, a statutory one, or a mixture of both. Individuals on both sides of this argument often point to the inadequacies the other may face when dealing with the problem. The claim most often levied against the courts is that they are too slow to react to the quickly changing technologies. While it is true that technology seems to be accelerating at break-neck speeds the ability of the courts to nevertheless

apply past principles as has been demonstrated here reveals that they too are able to adapt.

Further evidence of the adaptability of the courts is seen in the cases presented here involving the use of thermal imagers. Whereas courts initially interpreted the relationship with these devices in one manner eventually these interpretations were overturned by one that placed a greater premium on privacy. Such an interpretation may even be claimed to better embody the true spirit of the Fourth Amendment. What this set of cases further demonstrates, however, is that experiencing growing pains when it comes to technology is not a situation unique to the law's relationship with the internet.

Insofar as this work can speak to the relationship between statutory and judicial solutions to problems that may arise between the law and the internet there is already evidence of the fundamental role these two bodies play. As *Warshak* illustrates with respect to the Stored Communications Act (SCA), by claiming the portion of the statute granting police officers the power to request content information from ISP's to be unconstitutional, the courts play a vital role if the legislature becomes too overzealous in its attempts to adapt to new technologies. In this sense then it would appear that neither of these two bodies can deal with the changing technology alone, yet a more optimum balance may be created through give and take.

Given the reactive nature that the legislature and judicial branches are destined to have with respect to technology there is always bound to be some degree of lag between the emergence of a new or adapted technology and a governmental reaction to best apply the law to it. In this sense then the scholars critiquing these institutions are correct to a degree. Recent technological innovations have emphasized the importance of creating a

sound relationship between the law and the internet because this relationship is not as static as that between the law and previous technological innovations. Aerial surveillance is unlikely to yield any different results than the ones in *California v. Ciraolo* and as *Kyllo* made clear even very sophisticated thermal imagers will be judged in the same manner that older models are at least with respect to their warrantless use, unless they become mainstream devices. But the internet itself changes. It gains more functions and expands its reach in the lives of most individuals. Social networking once relegated to designated internet chat rooms can now be manifested in countless ways and not just from a computer but from a smartphone or a tablet. While phones have gained many of the functions of computers the opposite has also occurred with the advent of Voice over Internet Protocol (VoIP) technologies such as Skype allowing people's computers to function as telephones but using their internet connections rather than the telephone lines. Also gaining momentum is the idea of cloud computing wherein individuals are able to store a wide array of information from practically any device with an internet connection onto a remote server rather than on their own device. The concerns of those who fear the law may move too slowly for its own good become much more significant when one takes into account all of these and other recent technological innovations.

Is the law's current pace sufficient in order to deal with the burst of innovations listed above? There is no dearth of potential problems that may arise between the law and these new developments in cyberspace. Taking VoIP as an example, one solution the court may have for this technology may not be sufficient given that different pieces of software inherently function differently. Whereas most VoIP programs function using a client-peer model, comparable to that used by email servers, Skype functions using a

peer-to-peer model like various file sharing programs. Without getting too bogged down in the technical details of each it may be sufficient to observe how the courts have treated these models in the past.

On the one hand, in cases such as *Ganoe*, *Stults*, and *United States v. Perrine* peer-to-peer software has been found to essentially remove an individual's expectation of privacy to a large extent given that it allows others with the same software to access certain portions of one's computer. Courts have argued that installing such software amounts to disclosing such materials to a third party. One may then ask whether this interpretation of the fundamental model on which a certain program operates extends across other types of programs in which it is implemented. Alternately it was the client-server model that was in question in cases such as *United States v. Forrester* and *Warshak*. In these cases the court granted more protection to the material the defendants disclosed. Unlike in the peer-to-peer cases where content information was deemed fine to examine without a search warrant in the client-server cases the courts drew the line at gathering non-content information. In these cases, for instance, warrantless searches that merely gathered information regarding where emails were being sent to or where they were coming from were considered valid. To have gathered the content of the emails, however, would have been unconstitutional. Would the validity of a VoIP equivalent of a wiretap rely more on the manner in which peer-to-peer programs were previously judged or would they rely more on the overall function of the program, in this case as a telephone analogue.

The kind of situation outlined above is the type Kerr (2003) points to when he describes the importance of the perspective the law can potentially take when

encountering the internet. The external perspective would focus more on the model used while the internal perspective would essentially see a phone call. So one might then ask whether a warrantless search would be valid if someone were using a certain version of VoIP software as opposed to another. Would someone using Skype have the same decreased expectation of privacy as those who use peer-to-peer file sharing software? Would the content of their conversations be protected from a warrantless search or would it be admissible in court much like the content information gathered from file sharing software was? These kinds of questions are harder to answer and highlight the difficulties scholars have expressed the law may face with respect to the internet. These questions also highlight the potential benefit of explicitly classifying certain actions online as being worthy of a certain degree of protection based solely on how it compares to the physical world rather than how it functions mechanically as Kerr has posited.

Cloud computing though still in its infancy also has the potential to pose difficult questions. As cases such as *United States v. Simons* and *United States v. Angevine* demonstrated, company policies may reduce one's expectation of privacy when it comes to one's work. With people being able to access and store information on the cloud from work, home, an airport, or anywhere else, the expectation of privacy one has with respect to what they store on the cloud may pose some problems. Would the expectation of privacy remain the same to all the information one uploads to the cloud or could it perhaps shift depending on where the person was when they uploaded it? Can the *Katz* rationale survive even when the metrics upon which it is based become so mercurial to the point that they can no longer be gauged consistently? Perhaps the most pressing

technological innovation that needs to be addressed by the courts, however, relates to how to treat smartphones.

Orso (2010) and Engel (2010) have both considered the issues raised by smartphones with respect to the law. Whereas the Fourth Amendment cases surveyed here did not include questioning the search of a computer incident to arrest, such a search could now be said to be possible with the advent of smartphones, which can perform many of the same tasks as computers and can hold a large extent of private information. With smartphones it may be possible that an individual being searched incident to arrest receives a text message, an email, or has incriminating photos stored on their phone. Under such a scenario the question may be raised as to whether, similarly to *United States v. Meriwether*, the court may find that one sending a text message, an email, or a picture cannot be sure that the intended recipient will be the one that receives the message. Combined with the ability of files stored on the cloud to be accessed from smart phones and the importance of the degree to which the police can search a smartphone incident to arrest without a warrant is further magnified. Something upload from the privacy of one's home could then be indistinguishable in the eyes of the police from something uploaded from the office.

The *Katz* reasoning has indeed held fast against the different technological innovations it has faced so far yet, as the cases examined here have shown, its application involved cases where subjective and objective expectations of privacy were arguably easy to determine, either a defendant was at home or at work or they had waived some degree of privacy through installing some software or agreeing to some policy. When the border between home and work is blurred, however, as cloud computing combined with

mobile devices can do, which is further exacerbated with software whose privacy expectations remain ambiguous, the question of subjective and objective expectations of privacy become harder to determine, which directly undermines the applicability of the *Katz* rationale.

As the various new technologies are making clear the physical world and cyber world are becoming ever more interconnected. This increasing interconnectedness raises yet another problem about the efficacy of applying the law to the internet. Leary (2011) and Plourde-Cole (2010) both touched upon the issue that this melding of the two worlds may present. As the findings here have shown, courts have readily applied the *Katz* test to various internet related issues. The courts evaluated individuals' subjective and objective expectations of privacy yet how accurate can these judgments be?

The internet by its very nature is relatively new and there are undoubtedly many individuals that are ignorant as to the way in which it functions. Undoubtedly many people are not wholly aware of the difference between the peer-to-peer or client-server models. Surely there are some individuals who are genuinely unaware that through the installation of certain file-sharing programs they may be opening their computers to outsiders. Furthermore, as Leary points out, younger generations may have a wholly different view when it comes to an expectation of privacy than the older generation. What to the younger generation may seem more acceptable to do online would perhaps be eschewed by older generations. Both prongs of the *Katz* test may then be applied unfairly to someone who either has had little experience with the internet or who has grown up in a separate environment with the internet. If the rationale is then being applied unfairly is it worth it to keep applying it?

Illegally downloading music may be the norm for a large portion of the younger generation. They may feel perfectly safe doing so from the comfort of their homes while another large portion would refrain from such an activity since they more accurately understand the potential consequences of such behavior. Yet when asking whether society would find one to have an objectively reasonable expectation of privacy when downloading illegal music from one's home using a peer-to-peer program, those who do not know how such programs function may answer yes, while the court has consistently found that one does not have an objectively reasonable expectation of privacy when using such programs. This is perhaps the most difficult problem to answer when considering the efficacy of applying the law to the internet given that it is very hard to gauge what is truly objectively reasonable to society. This type of problem is further highlighted when it comes to the newer technologies such as VoIP and cloud computing. Many people may be willing to readily use such innovations yet it is unlikely that many will actively seek to learn how they actually function.

How is it possible then for a court to posit a credible objective expectation of privacy to such novel technologies? Yet it must be noted that this fault of the Katz test is not unique to the internet. With any technological innovation the court has had to guess to a large extent as to what society may or may not find reasonable. Nevertheless this line of reason may then seem to be the one that most puts the continued application of the *Katz* rationale into question. As the prongs of the *Katz* test become more difficult to determine concretely due to the unfamiliarity large portions of society may have with them, it may become harder for courts to claim to be able to accurately and justly continue applying the test. Yes the *Katz* rational has been consistently applied since it was first used in 1967

but that does not mean it will continue to be applied. Just as *Katz* overruled *Olmstead v. United States* it may itself be overruled by some rationale that more accurately fulfills the Fourth Amendment's purpose in the age of the internet. It is perhaps the types of hypothetical situations presented above that may eventually lead to a new method of interpreting the Fourth Amendment with respect to the internet.

Looking at the results of this inquiry may not seem all too surprising. Having been living in a world where the internet is commonplace for over a decade now it may seem like just another tool we use to make life more convenient, although it is a tool that is constantly getting better. Yet the internet has truly changed the face of the world and it is no wonder that many individuals were greatly concerned with how the law would interact with such an unknown entity that learns and grows. The fact that it is still learning and grown, however, reveals the importance of more concretely understanding the relationship between the law and the internet.

The findings presented here have been concerned with but a small portion of the much larger relationship between the law and the internet. Through this narrow focus a true consistency in approach among the courts was able to be more readily identified. While this approach grants greater insight into a small portion of this relationship, its generalizability with respect to the law in general may be harder to accomplish. It is here where other works can be used to supplement the findings presented in this case. For instance how the First Amendment or copyright law interact with the internet, among many other examples, are other areas of potential research that can grant a better understanding of the relationship as a whole.

With respect to the methodological approach taken here one benefit is that what is presented is a first-hand mapping of the reasoning courts have taken with respect to the scope studied. Obviously, however, this was not an exhaustive presentation of all the relevant cases on the subject, but this flaw can be easily remedied by merely increasing the sample size. The cases presented were rather varied, however, and still managed to demonstrate some consistency with respect to the reasoning strategies employed even across appellate circuits. Unfortunately the sample did not include Supreme Court cases involving the internet but that is perhaps to be expected given that not many such cases are likely to have reached such a level of deliberation. Another detriment of the approach undertaken here is that it does not take into account statutory attempts at reconciling the issues that may arise between the Fourth Amendment and the internet. Yet, as *Warshak* made evident, given that at issue is a constitutional question the courts' decisions can ultimately trump potentially troublesome statutes.

Ultimately the findings here have demonstrated several things. Primarily with respect to the regulability of the internet, the old principles are indeed applicable. The continued application of these principles is ultimately uncertain, however. As various authors above have noted, and the results here have shown, while there has been a consistency in the application of the *Katz* rationale this does not mean that there are problems with the way in which it is actually applied. Yet the work presented here if anything highlights how robust the legal system is given that it can be seen to steadily trudge along as the technological world runs circles around it. But it would appear that rather than being completely left in the dust by technology that the relationship between the law and technology is more like that of the tortoise and the hare. With its tried and

true principles the law can react and adapt to the world around it. By its nature the law will always lag behind but that does not mean it will become obsolete. Even in the rapidly evolving technological world courts can find links with the old to make some sense of the new. Yet the fact that the *Katz* rationale has survived its initial encounters with the internet does not mean that it will continue to do so.

References

Anon. 1997. Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication. *Harvard Law Review* 110, no. 7 (May 1): 1591-1608.

Anon. 1999. Developments in the Law: The Law of Cyberspace. *Harvard Law Review* 112, no. 7 (May 1): 1574-1704.

Bomse, Amy Lynne. 2001. The Dependence of Cyberspace. *Duke Law Journal* 50, no. 6 (April 1): 1717-1749.

California v. Ciraolo, 476 U.S. 207 (1986).

Engel, Joshua A. Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices. *University of Memphis Law Review*. 41:233-297.

Goldsmith, Jack L. 1998. Against Cyberanarchy. *The University of Chicago Law Review* 65, no. 4 (October 1): 1199-1250.

Grubins, Tamar R. 2008. Warshak v. United States: The Katz for Electronic Communication. *Berkeley Technology Law Journal*. 31, no. 1: 723-753.

Guest v. Leis, 255 F.3d 325 (6th Cir. 2001).

Johnson, David R., and David Post. 1996. Law and Borders: The Rise of Law in Cyberspace. *Stanford Law Review* 48, no. 5 (May 1): 1367-1402.

Katyal, Neal Kumar. 2001. Criminal Law in Cyberspace. *University of Pennsylvania Law Review* 149, no. 4 (April 1): 1003-1114.

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

Kerr, Orin S. 2003. The Problem of Perspective in Internet Law. *Georgetown Law Journal*. 93: 357-405.

Kerr, Orin S. 2010. Applying the Fourth Amendment to the Internet. *Stanfor Law Review*. 62: 1005-1049.

Kothari, Vivek. 2010. Autobots, Decepticons, and Panopticons: The Transformative Nature of GPS Technology and the Fourth Amendment. *American University Washington College Criminal Law Brief*. 6, no. 1:37.

Kyllo v. United States, 533 U.S. 27 (2001).

Leary, Mary G. 2011. Reasonable Expectations of Privacy for Youth in a Digital Age. *Mississippi Law Journal*. 80: 1033-1092.

Lessig, Lawrence. 1995. The Path of Cyberlaw. *The Yale Law Journal* 104, no. 7 (May 1): 1743-1755

Lessig, Lawrence. 1999."The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113.2 (1999): 501-549. Web. 23 Dec. 2010.

Litan, Robert E. 2001. Law and Policy in the Age of the Internet. *Duke Law Journal* 50, no. 4 (February 1): 1045-1085.

O'Connor v. Ortega, 480 U.S. 709 (1987).

Orso, Matthew E. 2010. Cellular Phones, Warrantless Searches, and the New Frontier of Fourth Amendment Jurisprudence. *Santa Clara Law Review.* 50: 183-224.

Plourde-Cole, Haley. 2010. Back to Katz: Reasonable Expectation of Privacy in the Facebook Age. *Fordham Urban Law Journal*. 38:571-628.

Sergent, Randolph S. 1995. A Fourth Amendment Model for Computer Networks and Data Privacy. *Virginia Law Review* 81, no. 4 (May 1): 1181-1228.

Smith v. Maryland, 442 U.S. 735(1979).

Strandburg, Katherine J. 2011 Home, Home on the web and other Fourth Amendment Implications of Technosocial Change. *Political Institutions: Constitutions eJournal* 5.46 (May 10): 101-165.

Tyson, Laura J. 2010. A Break in the Internet Privacy Chain: How Law Enforcement Connect Content to Non-Content to Discover an Internet User's Identity. *Seton Hall Law Review*. 40:1257-1298.

United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002).

United States v. Barrows, 481 F.3d 1246 (10th Cir. 2007).

United States v. Ford, 34 F.3d 992 (11th Cir. 1994).

United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008).

United States v. Hambrick, U.S. App. LEXIS 18665 (4th Cir. 2000).

United States v. Hechenkamp, 482 F.3d 1142 (9th Cir. 2007).

United States v. Karo, 468 U.S. 705(1984).

United States v. King, 509 F.3d 1338 (11th Cir. 2007).

United States v. Lifshitz, 369 F.3d 173 (2d Cir. 2004).

United States v. Meriwether, 917 F.2d 955 (6th Cir. 1990).

United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

United States v. Pinson, 24 F.3d 1056 (8th 1994).

United States v. Reyes, 798 F.2d 380 (10th Cir. 1986).

United States v. Simons, 206 F.3d 392 (4th Cir. 2000).

United States v. Slanina, 283 F.3d 670 (5th Cir. 2002).

United States v. Stults, 575 F.3d 834 (8th Cir. 2009).

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