
Eric Koester

Follow this and additional works at: https://repository.law.uic.edu/jitpl

Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation


https://repository.law.uic.edu/jitpl/vol24/iss2/3

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in The John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.
VOIP GOES THE BAD GUY: UNDERSTANDING THE LEGAL IMPACT OF THE USE OF VOICE OVER IP COMMUNICATIONS IN CASES OF NSA WARRANTLESS EAVESDROPPING

ERIC KOESTER

In December of 2005, the New York Times revealed that the Bush administration had previously authorized the National Security Agency ("NSA") to conduct surveillance on Americans without the court-issued warrants typically necessary for spying within the U.S.1 According to the New York Times reporters,

Under a presidential order signed in 2002, the [NSA] intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to Al Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.

The previously undisclosed decision to permit some eavesdropping inside the country without court approval was a major shift in American intelligence-gathering practices, particularly for the National Security Agency, whose mission is to spy on communications abroad. As a result, some officials familiar with the continuing operation have questioned whether the surveillance has stretched, if not crossed, constitutional limits on legal searches.2

While it is clear that the behavior of the NSA and the Bush administration represent a change in U.S. intelligence policy, the specifics and details of the program itself still remain unclear. The New York Times was purposely vague in its reporting of most of the program specifics stating: "some information that administration officials argued could be

2. Id.
useful to terrorists has been omitted.”

Without many specifics of this NSA domestic surveillance program, scholars, pundits, and politicians have been left to dissect this less-than-clear program in an attempt to understand what, if any, rules have been broken and whether the protections of Americans have been strained as a result. Certainly, reviews of the program have been frequent, yet no authoritative decision, source, or answer has been issued for the President’s decision. Instead, many Americans have simply labeled this as another political battle rather than a legal issue— with democrats and republicans each staked to their positions, primarily drawn down political lines. Some democrats in Congress are suggesting that the actions of the Bush Administration in the eavesdropping case are in fact criminal and that they warrant a full investigation. No formal actions, however, have been taken in the matter condemning this behavior. Two court cases, filed in early 2006, alleging the illegality of the NSA program have yet to be heard in court. Recently, some political analysts have suggested that any changes in the make-up of the Senate or the House could lead to a full review and formal actions against the President, possibly resulting in impeachment proceedings.

I. INTRODUCTION: THE NSA WARANTLESS SURVEILLANCE PROGRAM

A great deal has been written about the potential legality or illegality of the NSA domestic eavesdropping program. The Bush administration has vigorously defended its actions and has emphasized the effectiveness of the program in preventing potential attacks. According to the New York Times, “[s]everal officials said the eavesdropping program had helped uncover a plot by Iyman Faris, an Ohio trucker and naturalized citizen who pleaded (sic.) guilty in 2003 to supporting Al Qaeda by planning to bring down the Brooklyn Bridge with blowtorches.” On the other side, a number of well-respected legal scholars and individuals concerned with the protection of civil liberties have laid out numerous arguments against the program and its lack of a sound legal foundation.

The majority of the reviews into the NSA warrantless domestic eavesdropping program have centered on the broad themes of surveillance laws and the struggle between the protection of American interests

3. Id.
and the protection of American rights. These reviews are well placed and likely the most that can be expected without going into great depth into the specifics of each program and its aims.

A. NSA Domestic Surveillance of Voice over IP Communications

The aims of this paper are to review the legality of the NSA eavesdropping program in the context of an emerging communications technology, Voice over Internet Protocol ("VoIP"), also known as 'Internet Calling.' To do so requires insights into surveillance law and VoIP technologies generally to define the key characteristics of interest for this analysis.

There have already been at least two high profile suits brought in reference to the NSA program, and it is possible that others may well follow as more information becomes known. This paper postures that the strengths of VoIP technology would make it an attractive communication device for potential terrorists (and that particularly from 2001 to the present this device would have been used by technologically savvy individuals and promoted among those who wished to avoid detection of their communications). Therefore, it is quite possible that the NSA domestic eavesdropping program may involve listening to conversations or calls transmitted through these means, or possibly reviewing stored calls placed with VoIP technology.

How would a court analyze the actions of the NSA, particularly with respect to warrantless surveillance of Voice over IP communications? Given the unique nature of communications over the Internet, current definitions and rules may not fit into the framework of VoIP technologies. Therefore, this paper focuses on this question and, in the process, examines the future analytical framework for VoIP surveillance issues, in the context of the current NSA program investigations.

Voice over IP is a rapidly emerging technology that has begun to replace traditional phone service in homes and businesses. It is estimated that by 2008, there will be more than 24 million U.S. VoIP subscribers. Businesses around the world have already implemented

8. Voice over Internet Protocol is also called in the literature VoIP, Voice over IP, IP Telephony, Internet telephony, and Broadband Phone. For the purpose of this paper, we will primarily refer to the technology as VoIP or Voice over IP.

9. In addition, in the high profile case of Ali al-Timini, argued by Jonathan Turley, the Court of Appeals for the Fourth Circuit is presently reviewing whether it should remand the case back to the trial court to uncover whether NSA warrantless surveillance was used to monitor Ali by law enforcement officials.


VoIP for its voice communication needs. The Department of Justice has publicly expressed concerns about VoIP and its potential usefulness for terrorists.

Deputy Assistant Attorney General Laura Parsky told the Senate Commerce Committee that unregulated VOIP would be a ‘haven’ for terrorists unless the government forces connected providers to build special wiretapping capabilities into their systems.

‘If legal loopholes allow criminals to use new technologies to avoid law enforcement detection, they would use these technologies to coordinate terrorist attacks, to sell drugs throughout the United States and to pass along national security secrets to our enemies.’

Given these publicly expressed concerns by well-placed government officials over the use of VoIP by terrorists, the inexpensive costs of using VoIP technologies for international communications, the power of VoIP technology for advanced encryption, and the importance of avoiding detection by terrorists, VoIP technology must be viewed as a potentially dangerous communications tool if accessed by certain parties. Therefore, it is wholly plausible that the technology could have been monitored as part of the broader NSA eavesdropping efforts.

This paper first examines the technology of Voice over IP itself. VoIP does not represent one single technology, but the broader use of transmitting voice conversations over the Internet. This results in some differences in how regulations impact the differing uses of technologies. Fundamentally, Voice over IP represents a unique technology and does not fit cleanly within existing regulations. Much of the law on the books regulating communications and surveillance are somewhat outdated and were not enacted when technologies such as e-mail, voicemail, or Voice over IP were seen as an option. Therefore, this paper will address the technology itself and offer some insights into its unique nature.

Secondly, this paper explores the current landscape of surveillance law and regulation. In particular, it looks at the legal landscape in the context of the NSA domestic eavesdropping program and the concerns that have arisen as a result. Finally, it attempts to explain how the NSA program would be analyzed if it was discovered that the eavesdropping had been performed on VoIP communications. In this situation, as more and more communications users look to move from traditional telephone services to cheaper VoIP technology, an understanding of this area will be increasingly important. This analysis will provide some insight into future government regulations and the protections consumers should expect their legislators to enact.

B. ABOUT ELECTRONIC SURVEILLANCE PROGRAMS

The revelation of the NSA warrantless surveillance program, as well as its lack of detail, has done much to rouse an interest into the current technologies for suspect surveillance. Historically, wiretapping involved little more than a law enforcement official physically attaching surveillance equipment to a wire for monitoring.\(^\text{13}\) Today, with the use of more sophisticated digital telephone exchanges, in many cases, telephone tapping can be done remotely with the aid of a computer and support of the telephone service provider.\(^\text{14}\) This technique, however, will still generally require approved access to the system by the provider.

While it may appear in vogue to refer to “wiretapping” of a telephone call, it is probably no longer a fully accurate description of the surveillance process in an increasing number of cases, including surveillance of a VoIP communication. The advent of fiber optics and advanced switching technologies has made the process more sophisticated and potentially more extensive by going beyond electronic surveillance of telephone calls. These programs monitor voicemails, e-mails, Internet activity, and, in this case, VoIP transmissions. The Federal Bureau of Investigations (“FBI”) has a tool known as ‘Carnivore,’ which is able to scan through all of the e-mail traffic from any Internet service provider (“ISP”).\(^\text{15}\)

What is the specific process for a lawful surveillance program? The Communications Assistance for Law Enforcement Act (“CALEA”) of 1994 requires all carriers to have procedures and technology for intercepting calls, a policy that was recently expanded by the FCC to include VoIP providers that offer access to the traditional phone networks.\(^\text{16}\) After an individual is identified, a law enforcement official will obtain a court authorization (in most cases) and then the network carrier will record the required activity of the monitored individual. Depending on the type of information requested, the carrier can either simply record the information about each call/transmission (number, time, duration) or can in fact record the call/data transmission completely. It is then the responsibility of the law enforcement official to analyze the data, a process that has

---


14. Id.


become more automated and more high tech: "[d]ata coming in is run against up-to-the-minute database algorithms that look for patterns in calls or keywords that show relevance to current events and threats."\(^{17}\)

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 sets forth the procedures for government surveillance.\(^{18}\) These surveillance laws generally fall under two statutory schemes: The Electronic Communications Privacy Act ("ECPA")\(^{19}\) and The Foreign Intelligence Surveillance Act ("FISA").\(^{20}\) In addition, the 2001 Patriot Act expanded the reach of law enforcement capabilities.\(^{21}\) Specifically, it expanded the list of crimes which could use wiretaps to assist in the investigation. Furthermore, the Act permitted issuance of wiretap warrants in any court jurisdiction – rather than just the jurisdiction where the wiretap would take place, as had been the rule.\(^{22}\)

This paper examines in more detail each of these areas of the law with a particular focus on the relevant information for the surveillance of VoIP calls in the national security context. According to law professor Daniel Solove,\(^{23}\) both the ECPA and FISA provide guidance for the varied prongs of surveillance, and the respective protections each offer to the privacy of individuals. "Whereas ECPA regulates surveillance for domestic purposes (the investigation and prevention of crimes), FISA regulates the surveillance of foreign agents within the United States. Since [FISA] regulates foreign intelligence gathering, FISA provides a much looser set of protections than ECPA."\(^{24}\) Under ECPA or FISA, any government agencies engaging in surveillance activities are required to obtain a warrant from a U.S. district court for any domestic monitoring or from the FISA court for surveillance of foreign parties.


\(^{22}\) Id.

\(^{23}\) Daniel J. Solove is a professor of law at The George Washington University and has published extensively on issues of privacy and surveillance law.

1. **Electronic Communications Privacy Act**

The ECPA is organized into three parts: the Wiretap Act,\(^\text{25}\) the Stored Communications Act ("SCA"),\(^\text{26}\) and the Pen Register Act.\(^\text{27}\) According to Solove:

Title I, known as the Wiretap Act, deals with the interception of communications that are in transmission. Title II, known as the Stored Communications Act, covers the accessing of stored electronic communications and records. Title III of ECPA, known as the Pen Register Act, applies to pen registers and trap and trace devices, which record phone numbers or addressing information (such as the "to" and "from" lines on e-mail).\(^\text{28}\)

The ECPA specifically deals with three types of communications – wire, oral, and electronic. Here, we will focus primarily on wire and electronic communications.\(^\text{29}\) Wire communication references an "aural transfer" which is defined as a communication containing the human voice that is transmitted through wire.\(^\text{30}\) This definition would include both traditional telephone and Voice over IP calls. Electronic communication is the catch-all for all other types of non-wire or non-oral communications.\(^\text{31}\) This communication includes data, images, signals, or some video that may be transmitted through various transmission mediums.\(^\text{32}\)

An example of an electronic communication would be an e-mail.

The Wiretap Act provides primary guidance for traditional telephone monitoring. While it provides a great deal in terms of individual protections of privacy, the language in the statute does limit its scope substantially. One of the limitations is that the Wiretap Act only protects communications that are intercepted in transit – not those that are stored after transmission.\(^\text{33}\) Additionally, the Wiretap Act sets a high threshold for obtaining court authorization to monitor communications and limiting authority to certain government officials, only for a fairly specified range of activities.\(^\text{34}\) Of the three parts of the ECPA, the Wiretap Act is likely the most restrictive of the government, but also the most limited in its scope of applications.

---

26. Id. at §§ 2701-2711 (2000).
27. Id. at §§ 3121-3127 (2000).
29. Id. (according to Solove, the term oral communication "seemingly applies to communications intercepted through bugs or other recording devices that do not involve a wire transmission. So if the police attempted to place a bug in one's home to record one's dinner-time conversations, this would be an interception of an oral communication.").
31. Id. at § 2510(12).
32. Id.
34. Id.
The Stored Communications Act offers considerably lower protection to individuals than the Wiretap Act offers. According to Solove:

Regular warrants are required only to obtain the contents of communications in electronic storage for 180 days or less. If communications are stored over 180 days, the government can access them with an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order. There is no requirement for probable cause, only 'specific and articulable facts showing that there are reasonable grounds' to believe communications are 'relevant' to the criminal investigation. For remotely stored files, such as e-mails that have been downloaded and read, the DOJ contends that the government can access them with a mere subpoena, a radically different device than a warrant. Subpoenas do not require probable cause or judicial approval. As William Stuntz notes, federal subpoena power is 'akin to a blank check'.

The SCA defines electronic storage as "any temporary, intermediate storage" that is "incidental" to the communication as well as "any storage of such communication by an electronic communications service for purpose of backup protection of such communication." This definition is used for e-mails or other stored data files. However, as mentioned above, once an individual downloads or 'reads' an e-mail, the protection offered is even less – a 'remotely stored file' would only need a subpoena to be accessed. This raises an important issue for many privacy experts who note that the increased use of e-mails or other digital types of communication are given significantly lower protections under the SCA.

The most common type of surveillance done today is a pen register, also referred to as trap and trace. This type of surveillance produces a log that provides the numbers that were called as well as the date, time, and duration of the calls. It has also been used to monitor e-mail communications by listing the 'to' and 'from' addresses, the time, and the date of each e-mail. This does not, however, review the content of the e-mails. Since pen registers are usually much simpler to undertake (and to filter into a usable resource), 'trap and trace' are the most common source of surveillance, sometimes leading to a decision to pursue future interception of call or data content if the situation requires. The Center for Democracy and Technology ("CDT") estimates that there are tens of thousands of 'trap and trace' surveillance orders annually, while content interceptions only number in the thousands each year.

Regulated under the Pen Register Act, the protections for this type of surveillance are generally quite low. For a court to grant access to this surveillance information, the law enforcement official must certify that

35. Solove, supra n. 24, at 1283-1284.
"the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."\textsuperscript{38} Based on these standards, similar treatment has been applied to 'trap and trace' surveillance of e-mails and Internet addresses. "The USA PATRIOT Act expanded the definition of pen registers and trap and trace devices to apply to addressing information on e-mails (e-mail headers) and to Internet Protocol ("IP") addresses."\textsuperscript{39}

2. \textit{Foreign Intelligence Surveillance Act}

The Foreign Intelligence Surveillance Act’s review process is shrouded in secrecy and this secrecy has raised speculation as to its efficiency in oversight of government surveillance of foreign intelligence. In the wake of 9/11 and the intelligence failings, the Foreign Intelligence Surveillance Act has received greater scrutiny. FISA’s purpose has been to provide appropriate mechanisms for government agencies to obtain foreign intelligence, outside the bounds and restrictions of ECPA.\textsuperscript{40} It does not govern intelligence collection outside of the U.S.\textsuperscript{41} Instead, it was designed to provide some guidelines for the gathering of foreign intelligence by government agencies within the U.S. borders following questions of intelligence improprieties in the Nixon administration. FISA has extensively limited provisions to authorize monitoring of U.S. citizens.\textsuperscript{42}

FISA makes intentional electronic surveillance without proper authority punishable as a felony.\textsuperscript{43} "A person is guilty of an offense if he intentionally . . . engages in electronic surveillance under color of law except as authorized by statute."\textsuperscript{44} Authority for electronic surveillance is granted only after a review by a specially appointed court consisting of eleven district court judges. In addition, a three-judge panel hears appeals of any unsatisfactory decision against the government.

The Foreign Intelligence Surveillance Court ("FISC") is the court of review for these surveillance orders.\textsuperscript{45} FISA permits covert searches and electronic surveillance by the government based on review of the FISC. This review, under FISA, has a much lower standard for authorization of surveillance than surveillance of purely domestic actors. FISA's design is one that provides for a loose level of judicial oversight to the foreign intelligence gathering process.

\textsuperscript{38} 18 U.S.C. § 3123(a) (2000).
\textsuperscript{39} Solove, \textit{supra} n. 24, at 1287.
\textsuperscript{40} 50 U.S.C. § 1802 (2000).
\textsuperscript{41} \textit{Id.}
\textsuperscript{42} \textit{Id.} at § 1805(a)(3).
\textsuperscript{43} \textit{Id.} at § 1809.
\textsuperscript{44} \textit{Id.}
\textsuperscript{45} \textit{Id.} at § 1805(a).
FISA provides authorization for surveillance in two ways.\footnote{46} Under the first approach, warrants can be requested from the FISC prior to or within the first 72 hours of a surveillance effort.\footnote{47} According to FISA, a surveillance agent’s authority is contingent upon a showing of probable cause that the party under review is a “foreign power” or “an agent of a foreign power.”\footnote{48} This relatively expansive definition has led some to refer to the review as a cursory ‘rubber stamp.’ Under the second approach, the President may authorize surveillance efforts for up to one year without a court order.\footnote{49} This narrowly tailored exception requires that the surveillance must be monitoring communications “used exclusively between or among foreign powers.”\footnote{50} This exception was often used to monitor the diplomatic community. Under this approach, the Attorney General must certify that “there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.”\footnote{51}

II. UNDERSTANDING VOICE OVER IP TECHNOLOGY

A. THE PRACTICAL UNDERSTANDING AND DRAMATIC GROWTH

VoIP was a significant technological gain for the Internet. Specifically, Voice over Internet Protocol is the transmission of voice conversations over the Internet or any other IP-based network.\footnote{52} This differs from a traditional telephone system in that a general-purpose packet-switched network transmits voice data, instead of traditional dedicated, circuit-switched telephony transmission lines.

Many experts in the field of telecommunications have contended that implementation of Voice over IP will lead to significant advances in communications and greater cost savings for consumers.\footnote{53} Cost savings result from use of VoIP service due to the ability to transmit oral and data communications simultaneously over the same medium.\footnote{54} Without the need for multiple telephone and data lines in a home or a business, consumers ultimately see the cost savings. Accordingly, consumers have

\footnote{46} The President does not argue that he has used either of these methods to gain authorization for the NSA domestic surveillance programs.\footnote{47} 50 U.S.C. § 1805(a).\footnote{48} Id.\footnote{49} Id. at § 1802(a).\footnote{50} Id.\footnote{51} Id.\footnote{52} Federal Communication Commission, Consumer & Governmental Affairs Bureau, Voice Over Internet Protocol, http://www.fcc.gov/voip/ (accessed on Nov. 3, 2006) [hereinafter Voice Over Internet Protocol].\footnote{53} VoIPNews, VoIP Basics FAQ, http://www.voip-news.com/faq/voip-basics-faq/ (accessed Jan. 6, 2006) [hereinafter VoIP Basics FAQ].\footnote{54} Voice Over Internet Protocol, supra n. 52.
VOIP GOES THE BAD GUY

been able to pay a smaller fee for home or business telephone service by using VoIP through providers such as Vonage.

VoIP is able to operate over multiple technologies including satellite, wireless, cable, DSL, and IP over power line technology. As long as a user is able to connect to the Internet, VoIP technology will function. As a result, unlike use of the traditional telephone service providers, VoIP service is not likely to face legal issues of monopolization or substantial levels of government regulation. With the number of options available to provide VoIP service, many in the telecommunications industry view this area as the proverbial ‘Wild West,’ ripe for expansion.

Since 2004, VoIP services have been available that allow subscribers to use the service just as they would with a traditional telephone service. For example, a subscriber is able to keep their existing telephone number, make calls with the use of existing telephone equipment (with the addition of an adaptor), and receive calls with this service, all at costs that are less than traditional phone service providers. In addition, several providers now offer a monthly fee option that allows a subscriber to pay a flat fee for unlimited calling to the U.S., and some to Canada or selected countries in Europe or Asia. Moreover, if a subscriber is traveling in Europe or Asia, the service allows the user to simply connect to the Internet and make a call with their VoIP service without any additional charges being incurred by the subscriber or the recipient of the call.

Another advantage of VoIP technology is that it allows automatic routing of all incoming calls to a VoIP phone. Therefore, no matter where the user is, if there is an Internet connection, a VoIP phone has connection and the user will receive calls. This allows consumers to travel with a laptop and have immediate access to incoming calls. Call center agents have begun to convert to this technology as well. By using VoIP phones that are functional from anywhere, centers are able to allow operators to work from a home office or to move offices with little need for technology upgrades. Additionally, VoIP phones allow integration with various other Internet services. Integration includes video conversations message or data file exchange during a call to audio conferencing, or other types of communication flexibility. VoIP systems are also now

55. Some services such as Skype or GoogleTalk do not allow interfaces with traditional telephones and operate as purely PC-to-PC communications.
57. Id.
58. Id.
59. Id.
able to work over wireless networks.\textsuperscript{60}

B. Differing Approaches to Voice over IP Technology

One of the advantages to VoIP is the flexibility of its operations. As noted previously, VoIP does not require a particular type of Internet technology and can be transmitted over satellite, cable, or DSL, among others. Likewise, this technology allows a user to communicate with either a telephone or a PC as the user terminal.\textsuperscript{61} This results in different modes of VoIP operation: PC to PC, PC to telephone, telephone to PC, and telephone to telephone (via the Internet). Different modes of operation exist because all VoIP protocols are application layer protocols.\textsuperscript{62}

The result of this flexibility is that assigning definitions or rules to the technology remains more difficult than with traditional telephone service. Different options of VoIP communications may receive different treatment under the law. For instance, a VoIP call that can potentially connect to the traditional telephone network may now be required to be accessible for tracking on the 9-1-1 emergency network;\textsuperscript{63} however, this does not apply to all Voice over IP communications.\textsuperscript{64} Treatment of communications that travel from PC to PC may differ from communications that travel via the Internet, even though users speak to one another through traditional telephones. A 2005 rule referencing wiretapping issued by the Federal Communications Commission ("FCC") seems to have already created a divide in the VoIP community.\textsuperscript{65}

Earlier this month, the FCC said that VoIP providers must be prepared to accommodate law enforcement wiretaps, which are covered by the Communications Assistance for Law Enforcement Act (CALEA). The commission limited the requirement to 'facilities-based broadband Internet access service providers and VoIP providers that offer services permitting users to receive calls from, and place calls to, the public switched telephone network (PSTN).'\textsuperscript{66}

Many law enforcement officials have already complained that the decision will create greater difficulties for them,\textsuperscript{67} yet experts do question what impact such a split would have. This rulemaking decision could potentially lessen the standards required for monitoring PC-to-PC

\begin{itemize}
  \item \textsuperscript{61} \textit{VoIP Basics FAQ}, supra n. 53.
  \item \textsuperscript{62} \textit{Id.}
  \item \textsuperscript{63} \textit{Wiretap Rules Split}, supra n. 16.
  \item \textsuperscript{64} \textit{Id.}
  \item \textsuperscript{66} \textit{Id.}
  \item \textsuperscript{67} \textit{Wiretap Rules Split}, supra n. 16.
\end{itemize}
communications; thus, creating a situation where monitoring these communications would be viewed similarly to e-mail (subject to a lower standard). Under such a ruling, monitoring these communications (or stored versions of these transmissions) would require only a low level of oversight.

C. “WIRETAPPING” A VOIP COMMUNICATION

Monitoring a VoIP communication requires no physical access to telephone wires or lines because VoIP communications are digital packets of data; therefore, transmission of VoIP communications is different from traditional voice calls. Consequently, the equipment for call monitoring is somewhat more advanced than that used in traditional wiretaps. Nevertheless, the equipment is still easily accessible. Some industry insiders have said that any computer savvy teenager could likely order the tools needed to eavesdrop on a VoIP communication right on the Internet. As such, authorities with the assistance of Internet or VoIP providers can access VoIP communications with relative ease.

Perhaps more important to the concept of “wiretapping” or monitoring of VoIP communications is the relative ease of access to stored versions of VoIP calls, which may be reviewed under the SCA. Likely, the bigger issue surrounding the surveillance of VoIP communications is the ability to access stored versions of the call after it has been finished and resides on a server in cyberspace. This could create a situation where any call made over the Internet would place a perfect copy of the conversation into storage for future access by anyone having access to the server. In fact, in many cases, exact recordings of VoIP calls could be stored without the knowledge of the participants and accessed at a much later point. In this type of transmission, the ultimate recipient receives data-packets of voice communications transmitted over the Internet. Upon receipt, these data-packets are easily storable at any number of points along the transmission (from sender to service provider to recipient) often without the knowledge of the parties. Access to stored communications at any of the various points in the data path are likely the easiest way to monitor any individual's communications. This creates a unique legal issue involving VoIP communications, one that this paper explores in greater detail. What makes VoIP communications effective as a communications tool also makes it a dangerous gateway into an individual’s privacy.

68. This subject is discussed in greater detail in Section IV of this paper.
69. Hot Recorder, http://www.hotrecorder.com/index.asp?cdOp=BUYVOIP (accessed Oct. 24, 2006) (displaying an example of a Web site that sells equipment to record conversations over the Internet). The equipment uses two channels to record parties then merges them into a single file. This enables the user to store, share, and even search recordings.
Some hurdles do exist in the monitoring of these calls. Some systems offer advanced encryption to prevent monitoring, while other systems do not identify VoIP calls from other data transmission. The government has requested greater accessibility to VoIP communications for law enforcement surveillance, but it is somewhat unclear what this access entails and what monitoring it includes. One expert pointed to a looming privacy invasion due to increased use of the Internet for communications: “The solution of course is to capture all packets on the Internet, in the hope that you will ferret out the ones you need later with a court order.”

With powerful data-packet sniffing tools, it is possible that calls or data could easily be found in stored information. Ultimately, VoIP communications raise the issues of stored voice communications and the increased privacy concerns that may result.

How will courts view VoIP communications? A VoIP call is an “aural transfer” within the meaning of the Wiretap Act; therefore, any intercept of a VoIP call as it occurs, would be handled in the same manner as a traditional telephone wiretap. In the case of *U.S. v. Councilman*, the court ruled that temporary storage of an electronic communication during transmission, still left the communication subject to the protections of the Wiretap Act. This affirms that an intercept, even one that is done during temporary storage of a VoIP communication, is still subject to Wiretap Act protections.

Changes to the Wiretap Act and SCA under the 2001 PATRIOT Act may have muddied the water regarding review of stored VoIP transmission. Transmission storage is not temporary. Instead, storage is systematic on a network server, in some capacity, following transmission—often referred to as caching of data files. Prior to these changes under the PATRIOT Act, stored voice communications were treated differently than stored data (e-mail) communications. Monitoring of both voicemails and stored VoIP calls had previously fallen under the Wiretap Act, except for section 209 of the PATRIOT Act. This PATRIOT Act amendment deleted the clause “and such term includes any electronic storage of such communication” from the definition of “wire communication” under 18 U.S.C. § 2510(1). Additionally, an amendment to the SCA added the word “wire” to 18 U.S.C. § 2703, with respect to government access to store communications. In light of this change, § 2703 now

---

71. 18 U.S.C. § 2510 (2002) (defining “aural transfer” as “a transfer containing the human voice at any point between and including the point of origin and the point of reception.”).
72. 418 F.3d 67 (1st Cir. 2005).
73. *Id.* at 85.
states that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication." 75 This clearly divides stored communications and those in transmission.

As a result, it appears that the Wiretap Act covers VoIP communications in transit, but not VoIP communications in storage, including transient caching by service providers and systematic caching. Stored VoIP communications now fall under the SCA provisions.

Section 209 [of the PATRIOT Act] sweeps far more broadly than has been publicly discussed. What if the contents of ordinary telephone calls become stored as a matter of routine? This storage is likely to become far more common with the imminent growth of Voice over Internet Protocol ("VoIP") telephone calls. VoIP uses the packet-switching network of the Internet to connect telephone calls rather than the traditional circuit-switching used by established phone systems. 76

Under the changes from the PATRIOT Act, it now seems likely that a stored VoIP communication would be subject to lower protections than a contemporaneously monitored communication.

III. THE NSA EAVESDROPPING CONTROVERSY:
LEGAL ANALYSIS

Much has been written about the NSA Eavesdropping controversy. To focus the analysis of NSA eavesdropping on Voice over IP, a general examination of the NSA eavesdropping program is necessary. We still know little on the program's specifics. Recently, leaked information has revealed that powerful computer systems have been operating to uncover activity, words, data, and other information from suspected communications that would be of concern to the government. 77

Our analysis of the NSA program, from the information we do know, will be useful to apply to the focus of this paper: NSA eavesdropping of VoIP communications. We will examine the arguments postured by the U.S. Department of Justice and critics of the policy. 78 Finally, we will identify the key themes that are most important to the policy generally.

78. The analysis at issue is quite complex. Numerous papers and briefs by legal experts specifically address the issue in question. This paper is not intended to be a complete review, merely a summary analysis. Here, this paper only attempts to give an overview of the most important legal analysis in order to provide context for its application to VoIP communications. This paper will not make a determination as to whether or not the actions of the program were generally legal, but will lay forth key arguments that need to be addressed under the more specific facts at issue in this paper.
A. Current Legal Actions over the NSA Surveillance Program

While it is not clear what the outcome of lawsuits referencing the NSA warrantless domestic surveillance program will be and what, if any, course of action a court would take in such a trial, it is important to address the claims and understand the ramifications. We will examine these claims (or those of a similarly situated plaintiff) in light of a revelation that the communications in questions were done with Voice over IP technologies.

1. ACLU v. NSA

On January 17, 2006, the American Civil Liberties Union ("ACLU") challenged the actions of the NSA by filing a lawsuit in the U.S. District Court for the Eastern District of Michigan.\(^\text{79}\) The case, ACLU v. NSA/ Cent. Sec. Serv.,\(^\text{80}\) was levied by the ACLU in opposition to the warrantless domestic surveillance program authorized by the Bush administration.\(^\text{81}\) The ACLU complaint requests declaratory and injunctive relief.\(^\text{82}\) The five individuals\(^\text{83}\) and three organizations\(^\text{84}\) named as plaintiffs claim to have been in regular contact via telephone communication with people in or from the Middle East.\(^\text{85}\) As the suit alleges, based on currently available information, each of these parties reasonably suspects having been a target of the warrantless spying program.\(^\text{86}\)

The ACLU argued that the NSA violated the constitutional rights of the Americans targeted by this surveillance.\(^\text{87}\) According to the press release issued with the filing of the suit, the ACLU stated:

> In the legal complaint filed, the ACLU said the spying program violates Americans' rights to free speech and privacy under the First and Fourth Amendments of the Constitution. The ACLU also charged that the program violates the Constitution because President Bush exceeded his authority under separation of powers principles. Congress has enacted two statutes, the Foreign Intelligence Surveillance Act and Title III of the federal criminal code, which are 'the exclusive means by which elec-

---

80. Id.
81. Pl.'s Compl. ¶¶ 1,3 (Jan. 17, 2006); ACLU v. NSA/ Cent. Sec. Serv., 438 F. Supp. 754.
82. Id. at 59-60.
83. Id. at ¶¶ 12-16 (introducing plaintiffs Christopher Hitchens (Author/Journalist), James Bamford (Author/Journalist), Tara McKelvey (Author/Journalist), Larry Diamond (Democracy Scholar) of Stanford University and the Hoover Institution, and Barnett Rubin (Afghanistan Scholar) of New York University).
84. Id. at ¶¶ 8-10 (introducing plaintiffs Council on American-Islamic Relations, the National Association of Criminal Defense Lawyers, Greenpeace).
85. Id. at ¶ 56.
86. Id. at ¶ 60.
87. Pl.'s Compl. ¶ 195 (Jan. 17, 2006); ACLU v. NSA, 438 F. Supp. 2d 754.
tronic surveillance. . . and the interception of domestic wire, oral, and electronic communications may be conducted.\textsuperscript{88}

The ACLU has since moved for summary judgment in the case and awaits a verdict on this motion.\textsuperscript{89} The U.S. Department of Justice has so far declined to issue any formal comments on this pending litigation.

2. \textit{CCR v. Bush}

On the same day the ACLU suit was filed, the Center for Constitutional Rights ("CCR") filed a similar suit in the Federal District Court for the Southern District of New York. The suit alleges, "that the NSA Surveillance Program violates a clear criminal law, exceeds the president's authority under Article II of the Constitution, and violates the First and Fourth Amendments."\textsuperscript{90} Given the extensive communications CCR attorneys made with suspected Al Qaeda detainees, the CCR filed suit on its own behalf, as well as on the behalf of others similarly situated.

The complaint submitted by CCR raised similar concerns to the ACLU suit:

The Foreign Intelligence Surveillance Act explicitly authorizes foreign intelligence electronic surveillance only upon orders issued by federal judges on a special court. It expressly authorizes warrantless wiretapping only for the first fifteen days of a war, and makes it a crime to engage in wiretapping without specific statutory authority. Rather than seeking to amend this statute, the president simply violated it by authorizing warrantless wiretapping of Americans without statutory authority or court approval. As a result, the President violated his oath of office to take care that the laws of this nation are faithfully executed, and instead secretly violated a criminal prohibition duly enacted by Congress.\textsuperscript{91}

CCR raised particular concerns over the fact that some information typically subject to attorney-client privilege may have been subject to these wiretaps. The U.S. Department of Justice has so far declined to issue any formal comments on this pending litigation.

B. \textbf{Bush Administration & NSA Eavesdropping}

President Bush described the decision to allow warrantless surveil-

\begin{footnotes}
\item \textsuperscript{88} ACLU, \textit{ACLU Sues to Stop Illegal Spying on Americans, Saying President Is Not Above the Law}, \url{http://www.aclu.org/safefree/nsaspying/234866prsv20060117.html} (accessed Jan. 17, 2006).
\item \textsuperscript{89} Pl.'s Mot. for Partial Sum. Jugmt., \url{http://www.aclu.org/safefree/nsaspying/244531gl20060309.html} (accessed Mar. 9, 2006).
\item \textsuperscript{90} Center for Constitutional Rights, \textit{CCR Files Suit over NSA Domestic Spying Program}, \url{http://www.ccr-ny.org/v2/reports/report.asp?ObjID=IqViRA3n9&Content=693} (accessed Jan. 19, 2006).
\end{footnotes}
lance by the NSA as “crucial to our national security.”\textsuperscript{92} The Bush administration has defended the NSA warrantless surveillance program on the grounds of the inherent powers of the President as well as a claim of statutory authorization.\textsuperscript{93} These primary legal grounds of the administration are laid out in the December 22, 2005 letter from Assistant Attorney General William Moschella to the leaders of the House and Senate Intelligence committees,\textsuperscript{94} and reinforced by Attorney General Alberto Gonzale’s subsequent memorandum.\textsuperscript{95}

The Foreign Intelligence Surveillance Act of 1978 (“FISA”) bars surveillance of foreign persons in the U.S. without the approval of the U.S. Foreign Intelligence Surveillance Court.\textsuperscript{96} FISA specifically prohibits “electronic surveillance” unless authorized by statute: “A person is guilty of an offense if he intentionally . . . engages in electronic surveillance under color of law except as authorized by statute.”\textsuperscript{97} A violation of the statute subjects the violator to civil or criminal penalties.\textsuperscript{98} The U.S. Department of Defense (“DoD”) also sets forth regulations governing surveillance of U.S. persons.\textsuperscript{99} While not the law, compliance with the regulations is expected of the NSA.

The Bush administration claims the authority to approve these NSA surveillance programs, without warrants, is inherent in the powers granted to the President as commander and chief under Article II of the U.S. Constitution; this authority is supplemented under the September 18, 2001 Authorization for the Use of Military Force (“AUMF”). To provide a framework for our analysis of VoIP monitoring, each of these grounds will be individually examined.

1. \textit{Inherent Powers of the President as Commander and Chief}

The Bush administration argues that the President has the “inherent authority to conduct warrantless searches to obtain foreign intelli-

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{94} Id.
\item \textsuperscript{96} 50 U.S.C.S. § 1809 (LEXIS 2006).
\item \textsuperscript{97} Id.
\item \textsuperscript{98} Id.
\end{itemize}
\end{footnotesize}
gence information.” In the ongoing ‘turf war’ between Congress and the President over power, this argument represents the latest debate. The gathering of foreign intelligence is not an enumerated power of Congress under Article I of the Constitution, or under Article II as a power of the Office of the President of the United States. Consequently, questions arise. First, who is responsible? Second, who holds this power? Without an answer from the government’s chief referee, the U.S. Supreme Court, to adjudicate this disagreement, there is no final determination to this issue.

In a letter for the Office of Legal Affairs, the Bush administration laid out the claim that the President does retain constitutional authority — authority that has been upheld in reviews by courts in several circuits:

This constitutional authority to order warrantless foreign intelligence surveillance within the United States, as all federal appellate courts, including at least four circuits, to have addressed the issue have concluded. See, e.g., In re Sealed Case, 310 F.3d 717, 742 (FISA Ct. of Review 2002) (“[A]ll the other courts to have decided the issue [have] held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority . . . .”).

The present debate over the President’s inherent authority to conduct foreign surveillance is not new. The question of authority to conduct this type of surveillance has been a source of conflict between the President and Congress, but the passage of FISA in 1978 appeared to provide a guideline for foreign surveillance by the executive branch. In passing FISA, the Senate Judiciary Committee wrote:

The basis for this legislation is the understanding — concurred in by the Attorney General — that even if the President has an “inherent” constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance.

Some statements made on the Bush administration’s behalf have misplaced Congress’s role in regulating Presidential authority. Critics of the President’s position point out that the cases on which it relies, while addressing the issue of constitutional authorities, have not dealt with the question of Congress’s power to regulate that authority.

Regarding the question of Congress’s ability to regulate the President’s power to conduct foreign surveillance, the Congressional Research Service draws parallels to the oversight of domestic surveillance:

100. Legal Authorities, supra n. 95.
101. Ltr., supra n. 92.
While courts have generally accepted that the President has the power to conduct domestic electronic surveillance within the United States inside the constraints of the Fourth Amendment, no court has held squarely that the Constitution disables the Congress from endeavoring to set limits on that power. To the contrary, the Supreme Court has stated that Congress does indeed have power to regulate domestic surveillance. *United States v. United States District Court*, 407 U.S. 297, 323-24 (1972).\textsuperscript{103}

This analysis poses a difficult dilemma to reconcile. While much has been proffered regarding the President's inherent authority in this case, little has been offered to understand the administration's position on the role of Congressional oversight of the surveillance programs generally. Since the Supreme Court has previously authorized oversight on domestic monitoring, critics of the Bush administration's position question whether the Court would address the issue of Congress's ability to regulate foreign surveillance.

2. *September 18, 2001 AUMF*

In the wake of the attacks on September 11th, Congress passed the Authorization for Use of Military Force Against Terrorists ("AUMF"). It served as the basis for military action in Afghanistan to remove the Taliban that had been known for harboring terrorists involved in the 9/11 plots:

**AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.**

(a) IN GENERAL.—That the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.\textsuperscript{104}

The key language in this statute used by the Bush administration is Section 2(a) which authorized the President to "use all necessary...force against those nations, organizations or persons he determines planned, authorized, committed or aided the [9/11] terrorist attacks."\textsuperscript{105} This language has justified the NSA Surveillance program as well as actions including the detention of enemy combatants. The Bush administration

---


\textsuperscript{105} Id.
argues that the AUMF supplements his inherent authority for warrantless foreign intelligence gathering granted under the U.S. Constitution.

According to the language in FISA, intentional surveillance without authority is a felony except as authorized by statute. The crux of this Bush administration argument is that the authority to perform warrantless domestic wiretapping is implicit in the AUMF's authorization to use force – essentially, that surveillance done by the NSA falls within the authorization of force contemplated by Congress in this statute. This, according to the argument being raised, makes the NSA program exempt from liability with FISA due to the authorization of the activity under the AUMF. Under this reasoning, this type of warrantless foreign surveillance is to be understood as behavior contemplated in the category of “all necessary and appropriate force.”

Perhaps the most significant insights into the legal effect of the AUMF comes from the Supreme Court ruling in Hamdi v. Rumsfeld. In this case, Yaser Hamdi, an enemy combatant captured in Afghanistan and held in detention, claimed his imprisonment was in violation of 18 U.S.C. 4001, which reads: “No citizen shall be imprisoned or otherwise detained by the United States except pursuant to an Act of Congress.” Based on the language in Justice O'Connor's plurality opinion (joined by Rehnquist, Kennedy, and Breyer), the Court ruled that the AUMF was “an act of Congress” that authorized Hamdi's detention, and therefore his imprisonment was not in violation of 4001(a). Justice O'Connor determined that the detention of American and foreign citizens was “clearly and unmistakably” a “fundamental incident of waging war.”

Applying the Hamdi decision to the facts at issue in the NSA program, the question is whether this surveillance program is a “fundamental incident of waging war” which would fit within the authorization. More specifically, should this surveillance program also fit into the category carved out in the O'Connor opinion that includes the detention of an enemy combatant as an act of war? According to the Bush administration, this type of surveillance is part of such an effort authorized by the AUMF, rendering it exempt from FISA.
Critics of the Bush Administration have been unimpressed with the argument postured by the Justice Department using the AUMF as rationale for the establishment of this program. Tom Daschle (D), the former Senate majority leader, was particularly critical to the passage of the AUMF. According to Daschle, "the president has exercised authority that I do not believe is granted to him in the Constitution, and that I know is not granted to him in the law that I helped negotiate."116 Daschle is joined by other members of Congress in his criticism.117

Even some Republicans have expressed concern over the stance taken by the Bush administration in its use of the AUMF's broad grant of power to justify 'ancillary' government acts. During a Senate Judiciary Committee hearing, Lindsay Graham, a Republican senator from South Carolina, offered some reservations about pushing the boundaries of the resolution too far while questioning Attorney General Gonzales.

What I'm saying is that, if you came back next time or the next president came back to this body, there would be a memory bank established here and I would suggest to you, Mr. Attorney General, it would be harder for the next president to get a force resolution if we take this too far. And the exceptions may be a mile long.118

According to this thinking, were the administration to use this broad grant in excess of Congressional intent, future grants of authority may become much more narrowly tailored with more detailed provisions. This outcome would potentially limit the power of future administrations.

Other critics have raised issues regarding the norms of statutory construction in reference to the AUMF. Those critics note that according to traditional statutory interpretation, the 'general' terms of the AUMF should not be read to unnecessarily conflict with the 'specific' terms of FISA. In cases when a conflict exists between two statutes, the Supreme Court has held that "carefully drawn" statutes prevail over general statutes.119 Here, FISA provides a detailed legal guideline for domestic wiretapping, whereas the AUMF provides no express reference to wiretapping. Applying the AUMF to the NSA warrantless surveillance program can only be done through a broad interpretation of the force resolution. To many critics, this fact raises doubts to the applicability of the AUMF to the FISA exception and its rules governing domestic surveillance.

In addition, Congress has previously addressed the question of warrantless domestic wiretapping during wartime. Critics note that it is

presumptive of the Bush administration to read the actions of the Congress in passing the AUMF to have implicitly repealed itself on FISA. Such a repeal by implication has historically only been established by "overwhelming evidence" and "the only permissible justification for a repeal by implication is when the earlier and later statutes are irreconcilable." Given that many experts do not see FISA and the AUMF as irreconcilable, they find the argument of an implicit repeal of FISA's warrant requirement unconvincing.

Likewise, concerns have been raised regarding the potential conflict between the AUMF and the U.S. Constitution, specifically the Fourth Amendment. In reading the AUMF's grants broadly, the Bush administration appears to trump the rights proffered in the Constitution. Again, traditional statutory interpretation would utilize a reading without such conflicts, encouraging a reading consistent with the Constitution. \( \text{Kent v. Dulles} \) may offer guidance on this question, the Court refused to interpret the passport statute so broadly as to grant the President the power to withhold passports to applicants on basis of political affiliation. \( \text{[We]} \) hesitate to find in this broad generalized power [over passports] an authority to trench so heavily on the rights of the citizen, and thus construe narrowly all delegated powers that curtail or dilute fundamental rights.

Similarly, the Supreme Court has been hesitant to broadly construe statutory grants when addressing questions of rights of liberty for non-combatants during wartime. In two World War II era cases, the Court stopped short of permitting the President to detain U.S. citizens of Japanese heritage. \( \text{[We]} \) in \( \text{In Ex parte Endo} \) wrote "[i]n interpreting a wartime measure we must assume that their purpose was to allow for the greatest possible accommodation between those liberties and the exigencies of war." While the Bush administration points to the \( \text{Hamdi} \) decision for its justification of the extension of the AUMF, the other side has also found grounds for its criticism of the NSA program (which can be the case when looking to an O'Connor opinion for guidance). A distinction can be drawn between \( \text{Hamdi} \) as an enemy combatant and the non-combatants as referenced in the \( \text{Endo} \) case. Under such an interpretation,
the Court granted broader discretion under the AUMF in the case of *Hamdi* given his status as an enemy combatant.\(^{127}\) Under *Endo*, non-combatants subject to NSA surveillance would not be vulnerable to a broad reading of the AUMF without a more definitive statement by Congress.

### IV. MONITORING VOIP CALLS IN THE NAME OF NATIONAL SECURITY

Without additional facts about the NSA eavesdropping program, it is almost impossible to provide a complete answer to the question of whether the Bush administration acted properly. Therefore, to provide some guidance this paper will ‘fill in’ details of the program and offer proposed analysis based on current justifications and critiques of the broader surveillance law context.

#### A. Facts in Question\(^{128}\)

In June 2006, a network technician at USA, Datanet, an Internet Service Provider (“ISP”), came forward with information that a federal government agent had asked him for access to their systems to monitor “suspected terrorists.” According to the technician, in 2004 he provided access to the agent to monitor “e-mails, internet traffic, instant messaging (‘IM’) conversations, and Voice over IP conversations.” The NSA provided this ISP with a computer program to install on the network which “would monitor suspicious information or data as it crossed the network and would scan the stored server data nightly using a more ‘detailed algorithm’ to detect anything it may have missed.” These communications were sometimes monitored concurrently to the conversation and other times the system would access stored versions of the e-mails, IMs, and VoIP calls.

Suspected terrorist sympathizer, Nasir Mohammed, a U.S. citizen, used USA Datanet as his Internet Service Provider between 2004 and 2005. The government agent had told the technician that the system “only monitors the international communications, or those that do not have a definite destination.” According to the technician, approximately 10% of all e-mails, IMs, and VoIP calls do not have a way to identify its specific or its intended destination.

The technician was never given a warrant or any court order, but simply assumed the agent was authorized “because he said it was important in preventing another 9/11.” The government agent was identified

---

\(^{127}\) *Hamdi*, 542 U.S. at 507.

\(^{128}\) The facts in question here are not a real scenario but were created based on potentially likely facts.
as an employee of the National Security Agency ("NSA"). He claims his surveillance only targeted Mr. Mohammed's 'suspicious' and 'potentially dangerous' communications. The NSA claims this surveillance was part of its program to monitor international communications with domestic members of terrorist groups.

B. ISSUES FOR THE COURT

The court in the case of Mr. Mohammed will examine whether a crime was committed in violation of U.S. laws regarding the surveillance by the NSA.

A person is guilty of an offense if he intentionally —
(1) engages in electronic surveillance under color of law except as authorized by statute; or
(2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.129

The analysis by the court in this case will examine whether a punishable crime was committed in the surveillance of Mr. Mohammed's VoIP communications.

1. Fourth Amendment Protections of Mr. Mohammed

Does the surveillance of Mr. Mohammed violate the Fourth Amendment rights of a U.S. citizen? The Fourth Amendment of the U.S. Constitution states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.130

Beginning in 1967, the Supreme Court held that a wiretap was to be considered a "search" under Fourth Amendment.131 Monitoring of electronic data communications receives similar protections under the Constitution and therefore the analysis of 'wiretapping' a telephone call is similar to monitoring a VoIP call or a stored VoIP transmission.132 The result is that, in most cases, the government is required under the Constitution to obtain a warrant prior to engaging in surveillance activity.133 The surveillance by the NSA of Mr. Mohammed was done without

129. 50 U.S.C. 1809.
130. U.S. Const. amend. IV.
133. Katz, 389 U.S. at 357.
the authorization of a court issued warrant.

The key language of the Fourth Amendment is an express prohibition on "unreasonable searches and seizures." The question hinges on whether the actions in the NSA surveillance are in fact reasonable – a search without a warrant cannot violate the Constitution for a number of reasons, some of which will be discussed here. For this reason, the Bush administration has stated in its position papers that "the touchstone for review of government action under the Fourth Amendment is whether the search is 'reasonable'."

The touchstone issue here is reasonableness. In a reasonableness analysis, some of the factors to consider are: Did the government provide a sufficient reason for its failure to obtain a warrant? Was the search limited to only the data necessary? Was the timing important to protect individuals? Was the search limited in time? Were steps taken to protect others from unauthorized searches? Were other officials notified and informed of the actions? Ultimately, a court must make this determination on the basis of the specific facts at issue.

The facts of this case elicit serious concerns about the "reasonableness" of the government’s efforts. Its ongoing surveillance efforts appeared to leave room for monitoring completely domestic communications and individuals other than Mr. Mohammed. It is dangerous to allow the government to use a surveillance tool that monitors suspicious communications and scans anything it misses nightly. This tool is frightening because it could easily be used to trample on rights granted by the Constitution. This raises serious doubts as to the "reasonableness" of the surveillance under the Fourth Amendment given the facts in question; however, the government will likely make additional arguments to justify its surveillance of Mr. Mohammed, such as a national security exception, a border search exception, and proper consent for surveillance.

Several important cases have left open the issue of whether the government is allowed to conduct searches in cases of foreign intelligence surveillance. failed to resolve this issue and left the question unanswered regarding the gathering of foreign intelligence. In 1972, the Court decided in , that searches involving ‘purely’ domestic organi-

134. U.S. Const. amend. IV.
135. Legal Authorities, supra n. 95, at 37.
136. A review of “reasonableness” in the surveillance of Mr. Mohammed is somewhat nebulous in the same way as an analysis of the “reasonable person” standard in a negligence suit.
137. , 389 U.S. at 359.
izations could not be justified under a national security exception.\textsuperscript{138} The opinion expressly left the question of foreign intelligence collection unanswered.\textsuperscript{139} In \textit{Keith}, Justice Powell used a balancing test to weigh "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."\textsuperscript{140} As such the government will argue that in a case like Mr. Mohammed's, where an individual is being monitored for suspected ties to terrorism, the NSA is permitted to monitor his communications under an exception for national security. Justice Powell's language in \textit{Keith} served as the guideposts to enact FISA and to lower the Fourth Amendment protections in cases of domestic security. This is an important consideration, which the government has effectively balanced through FISA.

The government's argument is persuasive. The Supreme Court has not ruled on the issue, but in \textit{Keith}, it appeared to contemplate that such an exception could be applicable.\textsuperscript{141} With FISA's enactment, that exception seems to have been established. In the case of Mr. Mohammed, the government would need to submit evidence of its intentions to monitor him, including what his contacts were, what the aims of those contacts may have been, and what evidence was being sought. That these efforts are necessary to protect national security is reinforced by statements from the President and the Attorney General, both of whom apparently maintain full knowledge of the program's functioning details.\textsuperscript{142} While it certainly requires additional information from the government, under existing legal precedent, this reasoning does present some grounds to apply the exception.

A second argument can be made with respect to the Fourth Amendment under the border search exception. Consistent with the Fourth Amendment, the U.S. is allowed to perform searches at its borders "or its functional equivalent."\textsuperscript{143} As a result of this exception, the government will argue that it was monitoring data communications\textsuperscript{144} entering or exiting the U.S. at the functional equivalent of a border; that is, an informational border. A similar argument has been applied in the case of international postal mail. In that context, searches are allowed at any

\textsuperscript{138} See \textit{U.S. v. U.S. Dist. Ct. E.D. Mich.}, 407 U.S. 297, 322 (1972) (Powell, J.) (stating that the Court's decision did not address the issue that "may be involved with respect to activities of foreign powers or their agents.").

\textsuperscript{139} Id.

\textsuperscript{140} Id. at 314-15.

\textsuperscript{141} Id.

\textsuperscript{142} Legal Authorities, supra n. 95.


\textsuperscript{144} See \textit{U.S. v. Ickes}, 393 F.3d 501 (4th Cir. 2005) (using this exception in the case of computer data to permit government to search files stored on a computer hard drive).
point of entry from the postal service to the recipient or any U.S. post office responsible for delivery of international mail.\textsuperscript{145} This represents a colorable argument against Mr. Mohammed, but the monitoring software leaves some doubts as to the efficiency of monitoring only international communications. Such a question seems to open the debate about whether a post office or port of entry would be allowed to use its search exception in some purely domestic cases. It is troubling that in ten percent of cases, the NSA could well be monitoring a domestic communication. For an argument to be contemplated, those ten percent of communications should be excluded from the review process. Even with the exclusion, there are still concerns that the review is not truly monitoring a communication prior to entry, but in many cases, reviewing a communication after the fact. As a result, it is simply unconvincing to apply the border search exception to the case of Mr. Mohammed.

Finally, the government is likely to argue that it had the network technician's consent to access the network and to install the software used in the monitoring program. Under the theory that the ISP has authorized access to network monitoring, the government will argue that it did not require consent from the individuals using the ISP - only the ISP itself. Consent can be given by a party (in this case, the ISP) to effectively waive his or her Fourth Amendment rights.

Here, there is generally less protection provided under the laws for data transmissions when contrasted with voice transmissions. Again, this becomes a fact specific inquiry into the operations of the ISP. What is the language of the contract signed by each customer? Is there a provision by which the user grants the network the right to data traveling over the network? Does the ISP generally monitor the system? Does the ISP monitor content or simply usage? An important issue will be the terms authorized in the user agreement, which in some cases, could authorize monitoring by the ISP.

A Ninth Circuit court addressed whether consent by the ISP was sufficient to remove liability from a party requesting the data.\textsuperscript{146} The court determined that permission given by an ISP to access its customers' data was not enough to withhold privacy protections. Accessing data stored in the ISP's system is a violation of the Stored Communications Act when the party requesting the access knew or should have known its request was illegal.\textsuperscript{147} If successful, the government's argument that it obtained the technician's consent is a dangerous one. This is especially true as increased storage of Internet calls becomes the norm; however,

\begin{itemize}
  \item \textsuperscript{145} \textit{U.S. v. Ramsey}, 431 U.S. 606 (1977).
  \item \textsuperscript{146} \textit{Theofel v. Farey-Jones}, 359 F.3d 1066 (9th Cir. 2004).
  \item \textsuperscript{147} \textit{Id.}
\end{itemize}
that argument seems relatively weak given that NSA agents are cognizant of surveillance law.

To be clear, in the case of Mr. Mohammed, the Fourth Amendment question is first in the analysis. Here, the analysis does not end just because it is possible to conclude that the government may not have violated the Fourth Amendment. In order to avoid criminal liability, the NSA program must also comply with other constitutional limits and federal statutes.

2. *Was Proper Authorization for the Surveillance Obtained?*

*Does unauthorized surveillance of Mr. Mohammed violate 18 U.S.C. § 1809?* Without addressing the questions of constitutional authority or statutory authorization (as argued by the NSA and the Bush administration), the answer here is clear. The government violated this statute. It engaged in electronic surveillance under the statute in question by attempting to acquire wire communications and other information where Mr. Mohammed had a reasonable expectation of privacy. Mr. Mohammed is a U.S. citizen and thereby protected under the statute from such an invasion.

Surveillance of Mr. Mohammed could be authorized under various statutory schemes. Given the absence of authorization for the NSA program under FISA, the Wiretap Act, or the Stored Communications Act, the program violates the law.

It is unclear whether FISA authorization by the FISC would have even been sufficient, since Mr. Mohammed is a U.S. citizen and it is unclear whether only international communications were monitored. This is not an easily won argument for the government and a full review may well reveal that Mr. Mohammed should have received the full protections of ECPA. However, under the national security exception to the Fourth Amendment protections, based on the government’s proffered evidence of terrorism ties, authorization by the FISA court would have been sufficient in this case.

*a. FISA Authorization*

*Was the surveillance of Mr. Mohammed authorized under FISA?* The simple answer here is no. FISA requires review by the FISC within seventy-two hours following surveillance efforts or authorization for within one year by the Attorney General. The Bush administration has stated that, due to time constraints, it did not authorize the surveillance efforts under either of the two methods established in the Act.

---

149. *Legal Authorities, supra* n. 95.
Without following the procedures laid out under FISA, authorization for the program was not granted, and surveillance of Mr. Mohammed was impermissible.

b. Wiretap Act & Stored Communications Act

Was the surveillance of Mr. Mohammed authorized under the Wiretap Act? The surveillance of VoIP communications is subject to the requirements laid out in the Wiretap Act. These requirements include obtaining a warrant as well as the oversight of a Department of Justice official. Any concurrent monitoring of domestic VoIP calls would have required authorization under the Wiretap Act and evidence of ‘probable cause.’ The NSA program did not obtain court authority for its surveillance of VoIP communications. Since the program did not follow the procedures of the Wiretap Act, it could not obtain authorization.

Was the surveillance of Mr. Mohammed authorized under the Stored Communications Act? The review of stored VoIP communications is subject to the SCA, under the category of stored data. Under the SCA, requirements for reviewing stored data are much less stringent than under the Wiretap Act, often requiring only a subpoena. A showing of “probable cause” is not necessary. Failure to follow the procedures of the Stored Communications Act precluded authorization.

3. Is the Surveillance Program Authorized under Another Scheme?

a. Inherent Presidential Authority

The Bush administration argues that the President has inherent authority to authorize warrantless surveillance in cases involving foreign intelligence. It then uses this authority as grounds to claim that Congress cannot regulate the President on the issue, as it currently does through FISA. This effectively shows that FISA is unconstitutional. The President’s authority to order warrantless foreign intelligence surveillance within the United States is constitutional, as all federal appellate courts, including at least four circuits, to have addressed the issue have concluded. See e.g. In re Sealed Case, 310 F.3d 717, 742 (For. Int. Surv. Ct. Rev. 2002) (explaining that “all the other courts to have decided the issue held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information,” and further noting, “We take for granted that the President does

---

151. Id.
152. 18 U.S.C. §§ 2701-2711.
153. Id.
154. Id.
155. Legal Authorities, supra n. 95.
To claim an inherent constitutional authority for surveillance of Mr. Mohammed defeats the concept of governmental checks and balances. The Bush administration's analysis, which attempts to declare FISA unconstitutional, is misguided. It is inconsistent with analogous situations wherein Congress oversees the executive branch, as in current congressional regulation of domestic surveillance. Congress has the power to regulate foreign surveillance gathering within the U.S. under FISA, just as it has authority to set standards for purely domestic intelligence collection. The administration has presented no arguments explaining why this case should be treated differently or why the President should be permitted to act without oversight. Not only is that argument unfounded, it represents a dangerous precedent.

The administration is correct that the issue of warrantless wiretaps in foreign intelligence cases was addressed and upheld by several courts prior to the enactment of FISA. The Third Circuit held in *Butenko* that a warrantless wiretap was valid if the primary purpose was for gathering foreign intelligence information.\textsuperscript{157} Likewise, the Fifth Circuit in *Brown* upheld a wiretap on U.S. citizens' conversations, authorized by the Attorney General for foreign intelligence purposes.\textsuperscript{158} The D.C. Circuit Court reviewed a case that is factually closer to Mr. Mohammed's and involved monitoring the activity of a domestic organization with foreign ties. In *Zweibon v. Mitchell*, the court held that a warrant was required for the domestic surveillance of a domestic organization.\textsuperscript{159} The court was unconvinced that the domestic organization was a "foreign power or [its] agent"\textsuperscript{160} as is required under FISA.\textsuperscript{161} In light of a showing that an organization or individual was clearly a foreign power or agent, the court stated absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional.\textsuperscript{162} Notably, in each of these cases, the courts address the issue in the context of surveillance without FISA.

Since the enactment of FISA, there have been two major cases that have examined the question of its constitutionality. In both cases, the courts held that FISA was in fact constitutional.\textsuperscript{163} In *Duggan*, the court


\textsuperscript{157} *U.S. v. Butenko*, 494 F.2d 593 (3rd Cir. 1974).

\textsuperscript{158} *U.S. v. Brown*, 484 F.2d 418 (5th Cir. 1973).

\textsuperscript{159} *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975).

\textsuperscript{160} 50 U.S.C. § 1805(a)(3).

\textsuperscript{161} *Zweibon*, 516 F.2d at 604.

\textsuperscript{162} Id. at 633.

cited national security interests as grounds to uphold the lower privacy protection standards in FISA. In Nicholson, the court refused to suppress evidence collected under a FISA order, ruling that FISA did sufficiently protect the accused. These cases leave little doubt of FISA's constitutionality, and the Bush administration presents no evidence to the contrary, besides its assertion of inherent authority for foreign intelligence gathering that supersedes the need for a warrant.

Unfortunately, some of the criticism for this argument comes from the poorly reasoned position of the Bush administration. The administration has focused on whether or not the President has inherent authority in the Constitution to authorize warrantless wiretaps in cases of foreign intelligence. However, inherent authority is not the important question. Indeed the Administration points to the inherent authority argument in a string of cases prior to the enactment of FISA, which do not address the issue in question – Congress's role in regulating Presidential authority. The Administration also points to dicta in a 2002 decision, which stated, "[w]e take for granted that the President does have that authority," but the case law still fails to address the important issue. This "sleight of hand" is not only disappointing, but incomplete as grounds for arguing the inherent authority enables the President to conduct warrantless surveillance.

Ultimately, the Steel Seizure Case provides the appropriate framework for analysis of this question of Presidential authority. FISA was a collaborative effort, enacted by the President and Congress. Through it, Congress has created a systematic approach for authorizing wiretaps within the United States, in places where the Constitution and statutes are presumed to have their strongest effect. Congress has constitutional power to create Article III courts and has properly done so through FISA. On this issue of its oversight of foreign intelligence gathering through FISA, Congress has said that the President must abide by this law.

In the present instance, any attempt to supplant the protocols laid out by Congress and signed by the President is unconvincing. The Administration provides no evidence why Congress should be denied its oversight role here. Mr. Mohammed has been harmed by an executive official that clearly has not followed regulations, regulations set forth to protect the citizens of this country. The President's inherent authority argument is simply not sufficient to justify the NSA's warrantless wiretaps of Mr. Mohammed.

164. Duggan, 743 F.2d at 61.
165. Zweibon, 516 F.2d 594.
166. See generally U.S. v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980); Brown, 484 F.2d 418; Butenko, 494 F.2d 593; Zeibon, 516 F.2d 594.
b. Authority under AUMF

Under the AUMF, the “President is authorized to use all necessary and appropriate force” against those “nations, organizations, or persons [the President] determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons.” The two components of this presidential authority are that the force is “necessary and appropriate,” and that it is used against the parties included in the authorization.

Here, the monitoring of Mr. Mohammed fails both prongs of this test. First, wiretapping or reviewing stored VoIP communications obviously does not fit within the scheme of force contemplated by the AUMF. The Administration’s reliance on the language from the *Hamdi* decision is misplaced. The scope of the NSA program used against Mr. Mohammed is much broader than the Supreme Court appeared willing to accept in the *Hamdi* opinion. Moreover, *Hamdi* also set different standards for enemy combatants than for non-enemy combatants. Previously, the Court has been cautious in granting powers to the executive in times of war and no evidence suggests that the Court would view this situation differently now.

Likewise, reliance on the AUMF seems naïve, given the problems with statutory construction and the fact that Congress dealt with surveillance issues in the USA PATRIOT Act only one month following passage of the AUMF. Arguing to include warrantless surveillance into the September 18th Authorization creates a situation in which the government could justify almost any illegal or questionable behavior. Warrantless wiretapping by the NSA is simply incompatible with the AUMF and cannot be extended to be a “necessary and appropriate” force used against a U.S. citizen, such as Mr. Mohammed.

Secondly, it seems highly unlikely that Mr. Mohammed is a party contemplated by the AUMF. At a minimum, the government must prove that Mr. Mohammed has a substantial connection to September 11th. It is dangerous to argue that anyone who could act in a way that appears sympathetic to terrorists or sympathetic to individuals in the Middle East should now be deemed to be a party to the September 11th attacks and subject to surveillance under the AUMF.

C. Conclusion of the Court

The failure of the NSA to obtain proper authorization for its surveillance of Mr. Mohammed is in violation of 50 U.S.C. § 1809. It is plausible that Fourth Amendment protections may not be required in this case where serious national security interests can be shown by the govern-

ment, but this determination, that the government need not grant Mr. Mohammed protections from unreasonable search under the Constitution, does not remove the responsibility of the government to grant Mohammed some level of protection. These protections should have been granted to Mr. Mohammed under at least the standards of FISA and perhaps under those in ECPA.

Authorization was not obtained under FISA or under ECPA. It is unconvincing that the NSA program is exempt from regulation by Congress under the theory of the President's inherent authority under the Constitution. Even if the President has inherent authority to conduct foreign surveillance, it is a foundation of our democratic government to allow the Congress to initiate some limits to that power. Those limits were established in 1978 by FISA, which Congress passed and the President later signed.

Likewise, it is not convincing to argue that the NSA warrantless wiretapping program was authorized under the authority granted to the President under the AUMF. It seems counterintuitive to suggest that Congress granted this power and then one month later adapted surveillance laws under the PATRIOT Act. This argument fails to recognize that domestic surveillance is simply inconsistent with the Supreme Court's review of Hamdi as an enemy combatant.

The government acted improperly in monitoring the VoIP communications and analyzing stored data of Mr. Mohammed. This surveillance effort is in violation of 50 U.S.C. § 1809. The government did not obtain proper permissions to monitor the electronic communications of Mr. Mohammed and thereby acted in violation of the law.

V. CONCLUSION

The issue of the NSA warrantless surveillance is complicated, but what has certainly become clear is that law governing surveillance appears to be insufficient to keep up with advances in technology. As a result, it is important that legislators examine the topic broadly and look to changes that will serve a rapidly changing area that serves a crucial need in this country. At the same time, serious questions should continue to be raised regarding the NSA warrantless surveillance programs. It remains a delicate balance – protecting national security secrets while ensuring compliance with accepted legal standards. Unfortunately, the debate is unlikely to go away in the near term.

According to many experts familiar with the recent advances in technology involved in surveillance, the hypothetical case of Mr. Mohammed may have some threads that are very real. The new NSA surveillance program may well be an agile system able to analyze threats being transmitted over a range of communications options. In the case where
an international telephone call discusses bombing target sites or where an e-mail sent abroad uses language that raises a flag or where a stored voice call made of the internet reveals a plot to smuggle harmful materials into the U.S., a system may be able to point law enforcement officials to the parties involved. The problem is those "hits" that are not truly dangerous foreign intelligence and the impact on the rights granted to us under the Constitution. We may have a system that can focus our efforts on the bad guys, but assurances must be made to protect our citizens at the same time. This system may well be at hand and raises concerns, while possibly providing increased national security protections.

Technology is moving quickly and will continue to do so. But we cannot allow technology to dictate policy. In a system that makes a digital version of each "call", why would anyone need to wiretap a call? Our laws make it simpler to view a stored VoIP call than a regular call. Laws need to adapt and change more rapidly.

Questions remain. Unfortunately, the Bush administration's resistance to answer concerns and develop partnerships with others on key issues has left the public without comfort in the program. Many laypeople, prior to research or study of this issue, will remain convinced that the Bush administration was likely wrongly judged in the public arena. For these individuals, protection of national security techniques and secrets was more important than compliance with outdated regulations.

Today, I share major doubts and express serious concerns about the legality of the NSA's program. We are quickly entering an era where digital versions of every phone conversation, every e-mail, every Internet site visited and every activity may soon find their way into the computer memory banks. How can we feel certain that our government appreciates and protects our digital fingerprint in cyberspace? Without assurances that the government is not operating in a manner consistent with the laws enacted by our representatives, I am afraid of what privacies I can enjoy.

In conclusion, in a rapidly changing world, it is important that our laws be built to adapt quickly. Our security and our privacy depend on it.