1-1-2010

FISA Amendments Act 2008: Protecting Americans by Monitoring International Communications--Is It Reasonable?

Jessica LoConte

PACE UNIVERSITY
SCHOOL OF LAW

INTERNATIONAL LAW REVIEW
ONLINE COMPANION

Volume 1, Number 6 January 2010

FISA AMENDMENTS ACT 2008: PROTECTING AMERICANS BY MONITORING INTERNATIONAL COMMUNICATIONS; IS IT REASONABLE?

Jessica LoConte

"Those who can give up an essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

– Benjamin Franklin, Memoirs of the Life and Writings of Benjamin Franklin

INTRODUCTION

On July 10, 2008, President George W. Bush signed the Foreign Intelligence Surveillance Act of 1978 Amendments Acts of 2008 (FAA) into law. Days later, from the Rose Garden at the White House, he stated that the new law "will allow our intelligence professionals to quickly and effectively monitor the communications of terrorists abroad, while respecting the liberties of Americans here at home."[1] If only it were that

[1] Presidential Remarks on Signing the FISA Amendments Act of 2008, PUB. PAPERS 975 (July 14, 2008), *available at* http://www.presidential rhetoric.com/speeches/07.10.08.html.

simple, there would surely be less controversy surrounding the federal government's current surveillance practices. Undeniably, the government has a responsibility to prevent terrorist attacks, but the problem posed by FAA is that it allows for far greater governmental intrusion into the private communications of law-abiding Americans rather than effectively monitoring the communications among terrorists.

Specifically, the Fourth Amendment has long guarded the right of every American to be free from *unreasonable* searches and seizures of their property by government officials. This begs the question of whether the FAA provides *reasonable* means of guarding the safety of our Nation. Depending on who is asked, the answer to the question will be strikingly different. Former President Bush justified the new expansive surveillance program by delivering a dire warning to the American people, stating that just because "the terrorists have failed to strike our shores again [since 9/11,] [it] does not mean that our enemies have given up."[2] Moreover, Bush "vowed to do everything in [his] power to prevent another attack on our Nation."[3] Because President Barack Obama signed the FAA while he was a Senator, one can assume that he also believes the current surveillance program provides reasonable means to ensure the safety of the American people.[4] Accordingly, the United States' current surveillance practices under the FAA are likely to remain in effect until 2012.[5]

On the other hand, many Americans believe that this legislation is too intrusive, even if it was enacted in the name of national security. Senator Russ Feingold remarked, before the passage of the FAA, that the Act authorizes "the government to collect all communications between the U.S. and the rest of the world."[6] This could ultimately "mean millions upon millions of communications between innocent Americans

[2] *Id.*

[3] *Id.*

[4] Nat Hentoff, Op-Ed., *The Fourth Amendment Discarded*, WASH. TIMES, Jan. 26, 2009, at A19.

[5] The Act has a sunset provision. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 403(b)(1), 122 Stat. 2436 (2008).

[6] Press Release, Congressional Press Releases, Remarks of U.S. Senator Russ Feingold in Opposition to the FISA Amendments Act (July 9, 2008).

and their friends, families, or business associates overseas could legally be collected. Parents calling their kids studying abroad, emails to friends serving in Iraq – all of these communications could be collected, with absolutely no suspicion of any wrongdoing."[7] Senator Feingold is not alone in his opposition to the current surveillance program—many civil libertarians find the FAA incompatible with a free society. In response, the American Civil Liberties Union (ACLU) filed a lawsuit in the Southern District of New York on July 10, 2008, just hours after the FAA went into effect. The lawsuit, *Amnesty v. McConnell,*[8] challenges the constitutionality of section 702 of the FAA, and asks the court to issue a permanent injunction that would prevent the federal government from engaging in its current international surveillance practices.[9]

This note analyzes the FAA in light of Fourth Amendment jurisprudence and international privacy standards adopted by other nations. The note argues that surveillance, conducted in the manner authorized under the FAA, does not comport with the reasonableness requirement of the Fourth Amendment because the government can intercept potentially all international communications without any requirement that surveillance is targeted at individuals suspected of wrongdoing. The Supreme Court has balanced individual privacy rights with the government's need to protect the public numerous times, and never has the Court upheld a measure that invaded the privacy of so many law-abiding persons who had no connection to illegal conduct. Such dragnet surveillance techniques are not only fundamentally un-American, but are also in sharp contrast to how other countries have decided to strike the balance between individual privacy and national security.

Part I provides a background on section 702 of the FAA and highlights the controversy surrounding the Act by focusing on *Amnesty v. McConnell.*[10] Part II provides a very brief

[7] *Id.*

[8] No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf.

[9] Complaint §§ 108-10, at 42, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008).

[10] *Id.*

summary of Fourth Amendment jurisprudence, as interpreted by the Supreme Court, and its application in the national security context followed by an analysis of the FAA's constitutionality, in light of Supreme Court decisions. Part III discusses international standards relating to government surveillance practices with a detailed discussion of the latest decision issued by the European Court of Human Rights in the case of *Liberty v. United Kingdom*. This section is developed through an analysis of the FAA pursuant to the international standards set out in *Liberty*. Part IV proposes that while national security is an important government objective, it is also imperative to protect the freedom of U.S persons to communicate privately with non U.S. citizens located abroad. The current surveillance program under the FAA not only poses serious constitutional questions, but it is also incompatible with current international practice.

I. SECTION 702 OF THE FAA AND *AMNESTY ET AL. V. MCCONNELL*

A. Background on Section 702 of the FAA

Section 702 of the FAA grants authority to the Attorney General of the United States and the Director of National Intelligence (DNI) to jointly authorize surveillance of any individual reasonably believed to be located outside the borders of the United States, so long as that person is not a United States person,[11] in order to acquire foreign intelligence information.[12] Federal government officials do not attempt to circumvent the restriction on targeting only non-U.S. persons who are located outside the United States' borders because section 702 prevents the government from intentionally

[11] A "United States person" is defined as "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in Section 1101(a)(20) of Title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section. 50 U.S.C. § 1801(i)(2008).

[12] Foreign Intelligence Surveillance Act, *supra* note 5, § 702(a).

targeting a person located outside the United States if the primary purpose of such surveillance is to obtain information about a person located within the United States.[13] It is also important to remember that the FAA only authorizes the surveillance of foreign nationals who are located outside of the United States' borders. Pursuant to section 702, the government cannot intentionally target a United States person no matter where they are located.[14]

In order to conduct surveillance, the Attorney General and the DNI must provide to the Foreign Intelligence Surveillance Court[15] a written certification attesting that:

> (1) Targeting limitations have been followed;[16]
>
> (2) There are procedures in place that have been approved by the Foreign Intelligence Surveillance Court that are reasonably designed to "(I) ensure that an acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States; and (II) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States;"[17]
>
> (3) Minimization procedures will be used "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons;"[18]
>
> (4) "A significant purpose of the acquisition is to obtain foreign

[13] Foreign Intelligence Surveillance Act, *supra* note 5, § 702(b)(2).

[14] *Id*. § 702(b)(3).

[15] "The FISC consists of seven United States district court judges designated by the Chief Justice who meet in secret and are empowered 'to hear applications for and grant orders approving electronic surveillance and physical searches anywhere within the United States under the procedures set forth' in FISA. Similarly, FISA authorizes [sic] a three-judge appellate panel, designated by the Chief Justice. This special Court of Appeals consists of three district or court of appeals judges who hear appeals by the government when its applications are denied. From this panel decision, the government may appeal to the Supreme Court." William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U.L. REV. 1, 81-82 (2000).

[16] Foreign Intelligence Surveillance Act, *supra* note 5, § 702(g)(2)(A)(vii).

[17] *Id*. § 702(g)(2)(A)(i)(I)-(II).

[18] 50 U.S.C. § 1801(h)(1) (2008).

> intelligence information;"[19] and
>
> (5) The procedures used are consistent with the Fourth Amendment of the Constitution of the United States.[20]

If the FISC finds that the above requirements are met, then it will issue a warrant.[21]

Note that in order to obtain a warrant from the FISA court, it is not necessary for the Attorney General or the DNI to specify who the target of surveillance will be. In fact, the statute specifically states that any "certification made under this subsection [section 702] is not required to identify the specific facilities, places, premises or property at which an acquisition . . . will be directed or conducted."[22] Nor does the statute state that the government must have a reasonable belief that the targets of surveillance have a connection to criminal or terrorist activities. Although section 702 requires the government to adopt minimization procedures, the FISC is not provided with any details regarding the specific minimization procedures to be implemented, which limits the court's review of the ways in which intelligence agencies will use the intercepted intelligence data in the future.

Another provision that causes concern is section 702(g)(1)(B) of the FAA, which provides a temporary exception to the warrant requirement: surveillance may begin under the authority of the Attorney General and DNI without court authorization if "time does not permit the submission of a certification."[23] However, certification must be made to the Court no later than seven days after surveillance has commenced.[24] Lastly, section 702(i)(4)(B) allows the government to continue the surveillance practices, that the FISC found to be unlawful, while awaiting a decision from the Court of Review.[25]

---

[19] Foreign Intelligence Surveillance Act, *supra* note 5, § 702(g)(2)(A)(v).
[20] *Id*. § 702(g)(2)(A)(iv).
[21] *Id*. § 702(i)(3)(A).
[22] *Id.* § 702(g)(4).
[23] *Id*. § 702(g)(1)(B).
[24] *Id*.
[25] Foreign Intelligence Surveillance Act, *supra* note 5, § 702(i)(4)(B).

B. Amnesty v. McConnell*: A Case About the Constitutionality of Section 702 of the FAA*

1) The Facts and Procedural Posture of *Amnesty v. McConnell*

Just hours after the FAA became law, the ACLU filed *Amnesty v. McConnell* in U.S. District Court for the Southern District of New York on behalf of human rights organizations,[26] an international labor union,[27] journalists,[28] and defense attorneys,[29] all of whom allegedly rely on the ability to engage in confidential communications with individuals abroad in fulfillment of their professional obligations.[30] The defendants to this suit are the Director of National Intelligence,[31] the director of the National Security Agency,[32] and the Attorney General of the United States.[33] The plaintiffs filed a Motion in Support of Summary Judgment, the defendants replied with a Motion in Opposition to Summary Judgment; as of the date of this writing, the district court judge has not ruled on the motion.

---

[26] Amnesty International USA, Global Fund of Women, Global Rights, Human Rights Watch, the International Criminal Defence Attorneys Association, the Washington Office on Latin America, and PEN American Center. Complaint, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf.

[27] The international labor union referred to is the Service Employee International Union. *Id.*

[28] The Nation Magazine sues on behalf of itself and its contributing journalists Naomi Klein and Chris Hedges. *Id.* §§ 80, at 29.

[29] Attorneys Daniel N. Arshack, David Nevin, Scott McKay, Sylvia Royce. Complaint, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/faa_complaint_20080710.pdf.

[30] *ACLU Sues over Unconstitutional Dragnet Wiretapping Law*, STATES NEWS SERVICE, July 10, 2008, *available at* http://www.aclu-mn.org/home/news/aclusuesoverunconstitution.htm.

[31] Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008) (John M. McConnell, at the time of filing).

[32] Lieutenant General Keith B. Alexander, at the time of filing. *Id.*

[33] Michael B. Mukasey, at the time of filing. *Id.*

2) The ACLU's Argument that Section 702 is Unconstitutional

The ACLU argues that the FAA violates the Fourth Amendment, the First Amendment,[34] and Article III; however, for the purposes of this paper, I will focus on the ACLU's Fourth Amendment argument. The ACLU's primary concern with the new law is that the Act provides a means for the government to engage in "dragnet surveillance tactics"[35] because it expressly states that the government is not required to identify the facilities, telephone lines, e-mail addresses, places, premises, or property at which its surveillance will be directed in order to obtain a certified warrant from the FISA court.[36]

According to the ACLU, the lack of specificity in the surveillance warrant resembles "general warrants" that were issued by the English government which the Framer's specifically had in mind while drafting the Fourth Amendment and purposely meant to exclude because they lead to abuses of power by the State.[37] The ACLU argues that while the old FISA statute "generally foreclosed the government from engaging in 'electronic surveillance' without first obtaining an individualized and particularized order from the FISC,"[38] under the new amendment:

> [T]he government may obtain a mass acquisition order without identifying the people (or even the group of people) to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without specifying the particular communications to be collected; without obtaining

[34] The ACLU argues that the FAA violates the First Amendment "because it sweeps within its ambit constitutionally protected speech that the government has no legitimate interest in acquiring and because it fails to provide adequate procedural safeguards. Plaintiff's Memorandum in Support of Motion for Summary Judgment at 3, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/pdfs/safefree/amnesty_v_mcconnell_memosupportingsummaryjudgement.pdf.

[35] *Id.* at 1, 17, 21, 28, 41.

[36] *Id*. at 9 (referring to §702(g)(4)).

[37] *Id*. at 26.

[38] Complaint at 9, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. filed July 10, 2008) (quoting 50 U.S.C. § 1804(a)(2006)).

> individualized warrants based on criminal or foreign intelligence probable cause; and without making even a prior administrative determination that the acquisition relates to a particular foreign agent or foreign power. A single mass acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.[39]

The ACLU argues that through the use of mass acquisition orders issued by the FISA Court, the interception of communications by the executive branch violates both the Warrant Clause of the Fourth Amendment and the requirement of reasonableness. The ALCU argues that the Warrant Clause is violated because the FISC issues warrants without requiring the government to define either the location or the persons who will subject to surveillance. Second, the ACLU argues that even if the FAA surveillance practices do not violate the Warrant Clause, the FAA allows the government to engage in dragnet wiretapping tactics, which the Supreme Court has deemed to be unconstitutional on numerous occasions.

The ACLU also objects that the FAA does not explicitly state the minimization procedures that the government is bound to adopt under the statute, nor does it provide for adequate judicial oversight over the minimization procedures to be implemented by the executive branch. As a result of the FAA's failure to "place meaningful limits on the government's retention analysis, and dissemination of information that relates to U.S. citizens," large government databases can be

[39] Plaintiff's Memorandum in Support of Motion for Summary Judgment at 9, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008). The ACLU warns that the FAA creates the potential for the executive branch to intercept: "All telephone and e-mail communications to and from countries of foreign policy interest for example, Russia, Venezuela, or Israel – including communications made to and from U.S. citizens and residents. All telephone and e-mail communications to and from the leaders of the Pakistani lawyers' movement for democracy, with the specific purpose of learning whether those leaders are sharing information with American journalists and, if so, what information is being shared and with which journalists. All of the communications of European attorneys who work with American attorneys on behalf of prisoners held at Guantánamo, including communications in which the two sets of attorneys share information about their clients and strategize about litigation." *Id*. at 1-2.

created through the mass acquisition of international communications, and in the future those databases can be searched in order to find information about specific U.S. persons. [40]

3) The Government's Response in Defense of Section 702

The government's first argument is that the plaintiff lacks standing to file this suit; [41] for the purposes of this paper, however, I will assume that standing is proper and discuss the government's substantive arguments. The government argues that the FAA does not violate the Fourth Amendment because the surveillance authorized under the statute targets foreign persons who are located abroad, people who do not enjoy constitutional rights and protections.[42] The government urges the Court to assume that the surveillance agencies act in accordance with the targeting procedures specified in the FAA and do not engage in any type of reverse targeting of U.S. persons. The Government goes on to argue that when the communications of U.S. persons are collected incidental to surveillance targeted at foreign powers, a foreign intelligence exception to the Warrant Clause applies.[43]

The Government admits that because privacy interests of U.S. persons are implicated, the FAA must comply with the Fourth Amendment's reasonableness requirement, as the "underlying command of the Fourth Amendment is always that searches and seizures be reasonable."[44] The government argues that the FAA is reasonable because it provides the government with information regarding foreign threats to national security while protecting the privacy interests of U.S. persons who communicate with foreigners located abroad by requiring the Foreign Intelligence Surveillance Court to review all certifications for governmental compliance to the targeting

[40] Plaintiff's Memorandum in Support of Motion for Summary Judgment, *supra* note 39, at 20.

[41] Defendant's Memorandum in Opposition to Summary Judgment at 17, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/images/nsaspying/asset_upload_file531_37629.pdf.

[42] *Id.* at 34.

[43] *Id.* at 40.

[44] *Id*. at 33.

procedures and minimization procedures laid out in FAA.[45] The Government argues that requiring a warrant to be based on "individualized suspicion," which requires "identification of the persons, facilities, and communications to be surveilled,"[46] would place an unreasonable burden on intelligence gathering agencies and "impose a back-door warrant requirement" to international surveillance that is not necessary when the targets of surveillance are foreign powers located abroad.[47] The government asserts that any constitutionally protected privacy interests that the plaintiffs have in their communications are adequately protected *ex post* through minimization procedures.[48]

II. THE FOURTH AMENDMENT OF THE UNITED STATES CONSTITUTION IN THE NATIONAL SECURITY CONTEXT, *KEITH*, AND THE FAA

> 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.[49]

The framers of the Constitution were familiar with the horrible invasion of privacy that the English "general warrants" allowed, and they wished to prevent a similar abuse of power by the United States government when they ratified the Fourth Amendment.[50] At first, the Supreme Court required an actual trespass in order to establish that one's Fourth Amendment rights were violated by an unlawful search and seizure.[51] In time, however, in order to keep pace with

[45] *Id.* at 48-49.

[46] Defendant's Memorandum in Opposition to Summary Judgment at 53, Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/images/nsaspying/asset_upload_file531_37629.pdf.

[47] *Id.*

[48] *Id*. at 39.

[49] U.S. CONST. amend. IV.

[50] William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 3 (2000).

[51] Olmstead v. United States, 277 U.S. 438, 466 (1928).

modern technology, the Supreme Court extended Fourth Amendment protection to electronic surveillance in *Katz v. United States*.[52] While *Katz* is the seminal United States case discussing personal privacy rights in communications, like most Fourth Amendment jurisprudence, it focuses on an American individual's privacy rights in a criminal investigation rather than in the national security context. Because the "requirements for obtaining surveillance authority for the two threats are fundamentally distinct . . . [t]he Fourth Amendment cannot, and does not, provide even-handed guidance"[53] for assessing the constitutionality of a surveillance program such as the FAA.

A) Keith and National Security

The only Supreme Court case that deals with an individual's Fourth Amendment rights in a national security matter is *United States v. U.S. Dist. Court* (*Keith*).[54] In *Keith*, the Supreme Court addressed whether the Fourth Amendment required a neutral magistrate to issue a warrant prior to the executive branch commencing domestic surveillance for the purposes of national security.[55] According to the Court, "[t]he determination of this question requires the essential *Fourth Amendment* inquiry into the 'reasonableness' of the search and seizure in question, and the way in which that 'reasonableness' derives content and meaning through reference to the Warrant Clause."[56] Recognizing that "the *Fourth Amendment* is not absolute in its terms," the Supreme Court balanced "the duty of the Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."[57] The Supreme Court

[52] Katz v. United States, 389 U.S. 347 (1967). The *Katz* decision "implicitly recognized that the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." United States v. U.S. Dist. Court (*Keith*) 407 U.S. 297, 313 (1972).

[53] Banks & Bowman, *supra* note 50, at 9.

[54] 407 U.S. 297, 313 (1972).

[55] *Id.* at 309.

[56] *Id.* at 309-10 (emphasis added).

[57] *Id.* at 314-15 (emphasis added).

reasoned that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate that the executive officers of Government will act as neutral and disinterested magistrates."[58] Therefore, the Supreme Court declined to create a national security exception to the warrant requirement[59] and held that, in the case of domestic surveillance, even if surveillance is conducted in the interests of national security, prior judicial review was required in order for electronic surveillance to comport with the constitutional requirements under the Fourth Amendment.[60] The Supreme Court also made clear that the *Keith* decision pertained only to domestic surveillance programs, and did not address the question of whether the President has authority to conduct warrantless surveillance of foreign powers.[61]

B) Surveillance Must Always Comport with the Reasonableness Requirement

In *Keith,* the Supreme Court explicitly acknowledged that the requirements to obtain a warrant could be different in the national security context,[62] as the "exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime,"[63] yet regardless of whether the purpose of surveillance is for criminal investigation or to collect intelligence information, the use of electronic surveillance by the government always risks infringing on "constitutionally protected privacy of speech."[64] Therefore, the test of whether electronic surveillance conducted in the interests of national security comports with the

[58] *Id*. at 316-17 (emphasis added).

[59] *Id*. at 320.

[60] *Keith*, 407 U.S. at 324.

[61] *Id.* at 321-22 (stating: "[T]his case involves only the domestic aspects of national security. We have not addressed, and expressed no opinion as to, the issues which may be involved with respect to activities of foreign powers of their agents.").

[62] *Id*. at 322-23.

[63] *Id*. at 322.

[64] *Id*. at 320.

requirements of the Fourth Amendment is whether the surveillance is "*reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens*."[65]

Later decisions by the Supreme Court assessing the reasonableness of searches not based on suspicion have upheld statutes and regulations that invaded individual privacy where there was a legitimate government interest in public safety. Recently, in *Samson v. California*, the Supreme Court upheld a California statute that subjected all parolees to agree to be subject to a search or seizure without a search warrant and without any cause as a condition of their release.[66] The Supreme Court noted that such invasion of privacy of law-abiding citizens would not otherwise be tolerated under the Fourth Amendment. In 1995, the Supreme Court upheld the constitutionality of a school policy whereby all high school students who wished to play sports needed to consent to random drug tests not based on suspicion.[67] And, in 1989, the Supreme Court upheld another random drug and alcohol testing case for railroad employees because the search was narrow and all employees knew about the regulation.[68]

C. While It Is Unclear Whether the FAA Violates the Warrant Clause, the FAA Violates the Reasonableness Clause of the Fourth Amendment

A full discussion on whether the FAA violates the Warrant Clause of the Fourth Amendment is outside the scope of this note. However, in light of the Supreme Court's acknowledgement that Congress has the authority to relax the traditional warrant requirements in the case of surveillance conducted to protect national security, one can fairly assume that a court will be reluctant to declare the FAA as unconstitutional under the Warrant Clause. In *Keith*, the government conducted domestic surveillance without a warrant or any prior judicial approval, and this was unconstitutional

[65] *Id*. at 322-23 (emphasis added).
[66] 547 U.S. 843 (2006).
[67] Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995).
[68] Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).

according to the court, even though the surveillance was conducted for national security purposes. However, under the FAA, the intelligence agencies are required to obtain a warrant from the FISC in order to conduct surveillance. And even in the case where emergency surveillance commences without prior judicial approval for up to a period of seven days, the *Keith* opinion mentions that this would not constitute a *per se* violation of the Warrant Clause in the national security context. Accordingly, even if a court were to apply the same standards as did the *Keith* Court, the requirement of judicial oversight of executive branch surveillance under *Keith* is satisfied. Therefore, it will be assumed that the FAA does not violate the Warrant Clause of the Fourth Amendment, and the discussion of this note will concentrate on to the only remaining question of whether the FAA, which allows for the deviation from the traditional warrant requirement of particularity and suspicion, is "reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[69]

The government insists that preventing terrorism is the State's most important task; therefore, the FAA is reasonable.[70] But, this argument is conclusory and fails to take into account the constitutionally protected privacy interests of citizens, which the Supreme Court has articulated must be balanced against the government's need for intelligence information. Here, a careful analysis of both the necessity of surveillance information and privacy rights is warranted. In attempting to assess the proper balance between privacy and security, one should keep the words of Chief Justice Earl Warren in mind.

> This concept of 'national defense' cannot be deemed an end in itself, justifying any . . . power designed to promote such a goal. Implicit in the term 'national defense' is the notion of defending those values and ideas which set this Nation apart . . . . It would indeed be ironic if, in the name

[69] *Keith*, 407 U.S. at 322-23.

[70] Defendant's Memorandum in Opposition to Summary Judgment at 48; Amnesty v. McConnell, No. 08 Civ. 6259 (S.D.N.Y. July 10, 2008), *available at* http://www.aclu.org/images/nsaspying/asset_upload_file531_37629.pdf.

> of national defense, we would sanction the subversion of . . . those liberties . . . which [make] the defense of the Nation worthwhile.[71]

The government claims that it needs this surveillance data in order to protect the United States from terrorist attacks. The Supreme Court has recognized that government has a legitimate interest in promoting the safety of its citizens, and in the name of such safety, individual privacy rights sometimes must be compromised.[72] However, in each case where the Supreme Court has allowed suspicionless searches, the targets of such searches were limited to particular group of consenting people; in *Samson*, it was parolees, in *Vernonia School Dist.*, it was high school athletes who in the past used drugs heavily; and in *Skinner*, it was railroad employees who were well aware that they could be subjected to random drug and alcohol screenings as part of their job. Under the FAA, the government is not required to show any specific suspicion of wrongdoing, nor is the government required to certify that there is reason to believe the targets of surveillance are affiliated with terrorism. As the previous cases demonstrated, searches not based on suspicion are not *per se* unconstitutional, but when the scope of the FAA allows for the government to conduct a search of all electronic communications between non-consenting U.S. persons and non-U.S. persons located abroad, the government surveillance program becomes a fishing expedition.

If the FAA was enacted to help the government monitor terrorists' cells and hopefully prevent future terrorist attacks, then the government should be required to certify that its primary purpose in conducting the surveillance is to monitor the activities of terrorists located abroad, or to collect intelligence information that will prevent terrorist attacks on U.S. soil. Without any link between surveillance and wrongdoing, the requirement of reasonableness of the Fourth Amendment requires that the scope of suspicionless searches

---

[71] *Keith*, 407 U.S. at 332 (quoting United States v. Robel, 389 U.S. 258 (1967) (Warren, J., concurring)).

[72] *See id.*; *see also* Samson v. California, 547 U.S. 843 (2006); Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995); Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989).

be limited to a defined group of people, such as those whom the government knows to be affiliated with terrorism. Because the FAA does not limit surveillance to those suspected of wrongdoing and allows the interception of practically all communications between U.S persons and non-U.S. persons located abroad, it violates the Fourth Amendment's requirement of reasonableness.

A contrary result would suggest that when the Supreme Court decided *Samson*, it would have upheld a statute allowing the state of California to conduct warrantless and suspicion free searches of all its citizens, not just consenting parolees. Or, when it decided *Vernonia School District* and *Skinner*, the Court would uphold policies allowing the state to randomly drug test any citizen regardless of consent and regardless of any suspicion of wrongdoing. Here, the FAA allows the government to intrude into the private conversations of all U.S. persons who speak to non-U.S. persons abroad, who have not consented to such searches. Because the scope of such searches is overly broad, and is not based on any connection to wrongdoing, surveillance authorized under the FAA is unreasonable.

The government insists that even if the privacy rights of Americans are violated incidentally through its surveillance program, the minimization procedures provide an adequate remedy for such interference. However, the specific minimization procedures used by the government are classified as confidential,[73] so the people have essentially no way of knowing if their conversations are being intercepted, overheard and stored by the federal government.[74] To make matters worse, there is no judicial oversight into the specific minimization procedures that the intelligence agencies adopt pursuant to each warrant, and so the government quite possibly could create huge call databases, which could store the private conversations of Americans for years into the future.

Even though the Supreme Court has confronted many Fourth Amendment cases, none have specifically addressed the question that is posed in *Amnesty v. McConnell*: is the mass

[73] *In re* Sealed Case, 310 F.3d 728 n.16 (2002).

[74] Hentoff, *supra* note 4.

acquisition of communications data, which indirectly implicates U.S. persons' privacy rights, reasonable in relation to the end goal of preventing terrorism, regardless of whether a warrant is required in order to conduct surveillance targeted at foreign agents? In light of the lack of case law governing this issue,[75] I think it is helpful to take a step back and assess the current international standards governing communications surveillance in order to gain insight into how other nations have balanced the privacy rights of citizens versus a nation's need to protect its citizens from terrorism.

[75] On January 12, 2009, the Foreign Intelligence Surveillance Court released an opinion, dated August 22, 2008, where the court affirmed that surveillance conducted in accordance with the Protect America Act of 2007 (PAA), the predecessor to FAA, does not violate either the Warrant Clause of the Fourth Amendment or the requirement that all searches be reasonable. The PAA, similar to the FAA, allowed the government to conduct surveillance of foreign agents without requiring the target of surveillance to be specified. In assessing the constitutionality of PAA, the FISC boldly stated that there is a foreign intelligence exception to the warrant requirement, although the Court acknowledged that the Supreme Court has never explicitly declared that there was one. After having resolved the Warrant Clause issue, the Court admitted that the government's surveillance practices must comport with the Fourth Amendment's reasonableness requirement. Accordingly, the Court looked to the "totality of the circumstances" to determine the degree of intrusion into privacy the Constitution will allow. In attempting to construe the "totality of the circumstances" the Court started its analysis by declaring that "the interest in national security – is of the highest order of magnitude." To support this assertion, the Court cited a Supreme Court case which upheld a decision by the Secretary of State to revoke a citizen's passport on the ground that the holder's activities in foreign countries are causing or are likely to cause serious damage to the national security or foreign policy of the United States. It is beyond my understanding how dicta from this case, which involves one American who is suspected of wrongdoing, has any relevance in upholding the constitutionality of legislation which permits the surveillance of thousands or even millions of Americans. The infringement on personal liberty based on the suspected wrongdoing of a specific individual is very different than infringing on the privacy rights of all U.S. persons who communicate to non-U.S. persons located abroad. Since the Supreme Court has never analyzed the issue directly, nor has pronounced a foreign intelligence exception to the Warrant Clause, it is unclear whether they would agree with the reasoning of the FISC's latest decision. *In re* Sealed Case, No. 08-01 (FISA Ct. Rev. Aug. 22, 2008).

III. INTERNATIONAL LAW REGARDING GOVERNMENTAL SURVEILLANCE OF COMMUNICATION

A. Sources of International Law: Treaties and Custom

International law stems from a number of sources. The first step to resolving any international law question starts with consulting relevant treaties or binding resolutions.[76] In the event that such documents are not directly on point to the issue, one should next consider the role of international custom.[77] Lastly, judicial decisions may be consulted, because while they are not a direct source of international law, they can be helpful because such decisions reflect customary international law.[78]

The right to privacy is a well-recognized, "fundamental, though not absolute, human right."[79] Numerous international treaties establish that citizens are entitled a right to privacy in their communications. Beginning with Article 12 of the Universal Declaration of Human Rights (UDHR), which has been coined as "the modern privacy benchmark at an international level,"[80] there is language which states that "[n]o one shall be subjected to arbitrary interference with his . . . correspondence . . . . Everyone has the right to the protection of the law against such interference or attacks."[81] In addition, Article 12 of the American Convention on Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) incorporate similar language. According to Professor Charles H.B. Garraway, the key word is "arbitrary," meaning that "[t]argeted interference with the right to privacy in accordance with domestic law would not seem to run afoul of

---

[76] ANTONIO CASSESE, INTERNATIONAL CRIMINAL LAW 26 (2003).

[77] *Id.*

[78] *Id.* at 37.

[79] David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MARSHALL J. COMPUTER & INFO. L. 1, 8 (1999); *see also* Charles H.B. Garraway, *State Intelligence Gathering: Conflict of Laws*, 28 MICH. J. INT'L L. 575, 579 (2007).

[80] Banisar & Davies, *supra* note 79, at 8.

[81] Universal Declaration of Human Rights, G.A. Res.217A, at 12, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc A/810 (Dec. 12, 1948).

the human rights provision . . . although the targeting will need to be carefully designated so that it does not violate the prohibition against discrimination."[82]

The United States is not a signatory of the UDHR, nor did it ratify the American Convention on Human Rights. And while the United States finally did ratify the ICCPR in 1992, it did so with an express declaration that "the provisions of Article 1 through 27 of the Covenant are not self-executing,"[83] and went on to state that the declaration was meant to "clarify that the Covenant will not create a private cause of action in U.S. Courts."[84] Therefore, none of these provisions can be used to strike down the FAA as a violation of a treaty of the United States.

While it can be said that most nations recognize the right of privacy of their citizens, there are no international treaties that deal directly with international surveillance standards.[85] Accordingly, we must look to international custom to determine whether there is a rule of law that has developed from the "general and consistent practice of states."[86] Because virtually every nation conducts surveillance and intelligence gathering,[87] it is difficult to reconcile the individual privacy rights guaranteed to citizens who live in a country that ratified one of the above international treaties with international custom, which has historically tolerated surveillance by the State.

B. Liberty v. United Kingdom*: Balancing between Individual Privacy and National Security*

The recent European Court of Human Rights (ECtHR)

[82] Garraway, *supra* note 79, at 581.

[83] HENRY J. STEINER ET AL., INTERNATIONAL HUMAN RIGHTS IN CONTEXT 1142 (2007).

[84] *Id*.

[85] A. John Radsan, *The Unresolved Equation of Espionage and International Law*, 28 MICH. J. INT'L L. 595, 597 (2007).

[86] RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE U.S. § 102 (1987).

[87] Jeffrey H. Smith, *State Intelligence Gathering and International Law: Keynote Address*, 28 MICH. J. INT'L L. 543, 544 (2007); Glen Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 637 (2007).

decision, *Liberty v. United Kingdom*, suggests that international custom regarding surveillance is changing, as judicial decisions can be helpful in determining customary international law.[88] The international treaty directly implicated by this lawsuit is the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 8 of the ECHR provides:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of a country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[89]

This freedom to communicate without governmental interference is protected in the European Union as a human right, specifically "Article 8 of the ECHR establishes privacy in one's communications as a qualified, fundamental right."[90] Although the European Court of Human Rights has interpreted Article 8 to strictly prohibit the arbitrary interception of international surveillance data, in the interests of national security, Article 8's protections are not absolute.

During the 1990's the United Kingdom's Ministry of Defense operated an Electronic Test Facility that was capable of intercepting 10,000 simultaneous telephone calls, e-mails and faxes from Dublin to London and on to Continental Europe.[91] The United Kingdom's surveillance law at the time was The Interception of Communications Act 1985 (ICA),[92] which allowed for the interception of communications pursuant to a warrant. The warrants only allowed the government to

---

[88] CASSESE, *supra* note 76, at 37.

[89] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, 230.

[90] Alexander Diaz Morgan, *A Broadened View of Privacy as a Check Against Government Access to E-Mail in the United States and the United Kingdom*, 40 NYU J. INT'L L. & POL. 803, 817 (2008).

[91] Liberty v. United Kingdom, 2008 Eur. Ct. H.R. 58243/00, 2.

[92] The Interception of Communications Act 1985, c. 56 § 1, (Eng.).

physically intercept communications, not read them or listen to them. The "warrants covered very broad classes of communications, for example, 'all commercial submarine cables having one terminal in the UK and carrying external communications to Europe', and all communications falling within the specified category would be physically intercepted."[93] While it was necessary for the UK Government to obtain a warrant in order to intercept communications, "[t]he legal discretion granted to the executive for the physical capture of external communications was . . . virtually unfettered."[94]

After obtaining the warrant, the Secretary of State was required to issue a certificate describing the classes of communications that could be "extracted from the total volume of communications intercepted under a particular warrant."[95] The certificates did not need to specify the targets of surveillance, but rather just label the categories as either relating to "national security," "preventing or detecting serious crime," or "safeguarding the economic well-being of the United Kingdom."[96] "National security" meant any activities "which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means."[97] In determining whether a warrant should be issued for such surveillance, the ICA required the Secretary of State to find that a warrant was necessary because the information could not reasonably be acquired through other investigative methods.[98] These two steps formed a "certified warrant."[99] After the "certified warrant" was issued, the judiciary's role in the process ended, and it was up to the state officials to come up with keyword search terms so that an automated search engine could filter the intelligence data collected.[100] The ICA required the

[93] *Liberty*, 2008 Eur. Ct. H.R. 58243/00, 12.

[94] *Id*. at 18.

[95] *Id*. at 12.

[96] *Id.*

[97] *Liberty*, 2008 Eur. Ct. H.R. at 5 (citing 1986 Report of the Commissioner).

[98] The Interception of Communications Act 1985, c. 56 § 2(3) (Eng.).

[99] *Liberty*, 2008 Eur. Ct. H.R.at 12.

[100] *Id*.

executive to create rules designed to promote the "minimisation of the interference with privacy."[101]

Despite the minimization procedures, however, Liberty (a British civil liberties' organization based in London), British Irish Rights Watch, and the Irish Council for Civil Liberties (both Irish civil liberties' organizations based in Dublin) commenced a lawsuit against the United Kingdom of Great Britain and Northern Ireland, claiming that the government infringed upon their privacy rights by physically intercepting virtually all international communications, including applicant's privileged and confidential communications.[102]

The applicants argued to the Court that the Government's interception of private communications was not proportionate to any legitimate aim of protecting national security, since "the 1895 Act permitted interception of large classes of communications for any purpose, and it was only subsequently that this material was sifted to determine whether it fell within the scope of a [certified] warrant."[103] The Government submitted that "in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication physically intercepted" under such a warrant.[104] The Government said that in the interest of national security, it could not disclose how it filtered the physically intercepted data as "[i]t would enable individuals to adapt their conduct so as to minimize the effectiveness of any interception methods which it might be thought necessary to apply to them."[105] However, the Government urged the Court to trust that the Government had safeguards in place to ensure that communications were not surveilled arbitrarily.[106]

The European Court of Human Rights was unconvinced by the government's promise to conduct surveillance in a manner

---

[101] *Id*. at 13.

[102] *Id.* at 12. Applicants were lawyers who were in regular contact with clients abroad and provided legal advice through electronic means.

[103] *Liberty*, 2008 Eur. Ct. H.R. at 13.

[104] *Id.* at 14.

[105] *Id*.

[106] *Id.*

that was "in accordance with the law"[107] and held that there was an actionable interference by the government's data mining practice. The ECtHR stated that, "the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied;"[108] therefore, the UK's surveillance program amounted to an "interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."[109]

The ECtHR next stated that the interference in privacy was justified because the surveillance was necessary in the interest of national security; the only question that remained before the Court, therefore, is whether the government's interception of private communications was in "accordance with the law."[110] The ECtHR held that in order for an international surveillance program be in accordance with the law, it is "essential to have clear, detailed rules on interception of telephone conversations . . . [so that it] give[s] citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures."[111] The Court described certain "minimum safeguards" that must be explicitly spelled out in any international surveillance statute in order to be in "accordance with the law." These safeguards included:

> (1) the nature of the offences which may give rise to an interception order;
>
> (2) a definition of the categories of people liable to have their telephones tapped;
>
> (3) a limit on the duration of telephone tapping;
>
> (4) the procedure to be followed for examining, using and storing the data obtained;
>
> (5) the precautions to be taken when communicating the data to other parties; and

[107] *Liberty*, 2008 Eur. Ct. H.R. at 20.
[108] *Id*. at 16.
[109] *Id*.
[110] *Id*. at 17.
[111] *Id*. at 18.

> (6) the circumstances in which recordings may or must be erased or the tapes destroyed.[112]

The ECtHR described the government's authority to intercept data under the Interception of Communications Act 1985 as "virtually unfettered,"[113] and therefore held that the ICA was in violation of Article 8 of the ECHR. To remedy this intrusion into private communications, the Court declared that "[e]veryone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."[114]

C. The European Court of Human Rights Would Declare the FAA Unlawful

In light of *Liberty v. United Kingdom*, if one were to hypothetically challenge the FAA in the European Court of Human Rights, it is unlikely that the Court would uphold the FAA as a lawful surveillance program because the scope of authority granted to the intelligence agencies to intercept and examine private communications is close to limitless. Moreover, the law does not clearly state how data mining will be conducted in order to prevent abuse of power by the executive branch. In addition, because there is no public disclosure about the minimization procedures that the intelligence agencies are required to follow, there is no way for the public to know whether their conversations are likely to be the subject of such an invasion..

Like the plaintiffs in *Amnesty v. McConnell*, the plaintiffs in the ECtHR lawsuit were civil rights activist organizations who claimed that the government infringed upon the privacy rights of all citizens through their surveillance program, which had the effect of physically intercepting almost all international communications. The plaintiffs claimed, similar

---

[112] *Liberty*, 2008 Eur. Ct. H.R. at 18.

[113] *Id.*

[114] *Id.* at 20. It is interesting to note that the remedy created by the Court's holding in *Liberty* is in direct conflict with the retroactivity immunity that the FISA Amendments Act of 2008 grants telecommunication providers. Foreign Intelligence Surveillance Act, *supra* note 5, § 801.

to the ACLU, that the government's intrusion into the privacy of all citizens was not proportionate to the goal of national security.

Liberty sets out a two-prong test in order to determine whether surveillance which interferes with the private communications of citizens is in "accordance with the law." Accordingly, surveillance must be foreseeable, meaning that a surveillance statute must provide clear, detailed rules about surveillance procedures so that it gives citizens an indication as to the circumstances in which their conversations will be monitored; such procedures must comply with certain minimum safeguards.

1) Foreseeability

The ECtHR struck down the Interception of Communications Act 1985, even though surveillance was conducted pursuant to a warrant, because the judicially issued warrants were so vague and all-encompassing that, in the eyes of the ECtHR, they granted too much discretion to intercept and dissect private communications. The ECtHR found that the ICA failed to prevent an abuse of power by the state and failed to allow citizens the opportunity to know when their communications would be subject to a search. The ICA did not require the intelligence agencies to specify the particular individuals or places to be targeted, but rather warrants would be granted if an executive official certified that such surveillance related to national security, and that such surveillance was necessary because the information could not reasonably be acquired through other means.

Similarly, under the FAA, the Foreign Intelligence Surveillance Court will issue a warrant for surveillance as long as the Attorney General and Director of National Intelligence certify that a significant purpose of the acquisition is to obtain foreign intelligence information. Other than the requirement that officials cannot intentionally target U.S. persons, there is no requirement that the surveillance be targeted at any specific person or place. Accordingly, nothing in the FAA prevents the government from abusing its power in conducting surveillance for purposes other than preventing terrorism. The executive branch is given broad discretion to monitor international

communications, so long as the ascertaining of foreign intelligence information is a significant purpose of the surveillance.

Theoretically, when the two statutes are compared, the FAA allows for even more interception of international communications, as there is no requirement that the United States government certify that such surveillance is necessary. Perhaps this means that the government can:

> [E]ngage in the wholesale collection of *Americans'* international communications . . . for example, knowingly and intentionally collect all communications between the New York and London offices of Amnesty International . . . Indeed, under the FAA the government can obtain *all* communications between New York and London so long as the ostensible targets for this mass acquisition are non-U.S. persons believed to be in the United Kingdom.[115]

By giving the government such broad discretion, there is no way for Americans to adjust their behavior so that they are not the subject of surveillance, other than perhaps deciding to never speak to any non-U.S. person abroad through the use of electronic communication equipment. It is highly unlikely that the ECtHR would uphold a surveillance program as expansive as the FAA, because the FAA grants the United States federal government the authority to intercept, inspect and store all international conversations that occur through electronic means, without a showing that such surveillance is necessary in the interests of national security. In addition to employing dragnet surveillance tactics, a surveillance program similar to the FAA would not pass muster in the ECtHR as it does not adequately put citizens on notice that their communications are being monitored.

The government in the ACLU case urges the Court to assume that the Executive Branch will abide by the regulations set forth in the FAA in order to comply with its prohibition against reverse-targeting and have in place certain minimization procedures designed to protect the privacy of U.S. persons whose communications are intercepted incidentally.

---

[115] Plaintiff's Memorandum in Support of Motion for Summary Judgment, *supra* note 39, at 39 (emphasis added).

When the UK government attempted this "just trust us" argument, the ECtHR was unconvinced that such a large degree of executive discretion would result in non-arbitrary intrusion into communications. In this vein, and remembering what the *Keith* court said about the nature of the executive branch, the court in *Amnesty v. McConnell* should be very hesitant to defer to the executive branch such a degree of unregulated discretion without judicial oversight.

2. Minimum Safeguards

The FAA fails under the minimum safeguards analysis of *Liberty* as well. The ECtHR specifically held that any surveillance statute must specifically state the "nature of the offense" which gives rise to an interception order, however, the FAA does not require the government to believe that the target of surveillance is related even remotely to criminal or terrorist activities. If the target of the surveillance is an unknown foreign agent, who intelligence agencies have no reason to believe is engaged in criminal or terrorist activities, what is the nature of the "offense" in such a situation? Surely, U.S. persons engaging in communications with non-U.S. persons cannot be an "offense."

The ECHR would also require a surveillance statute to explicitly state the categories of people liable to have their telephone lines tapped, which may mean people who communicate with known or suspected terrorists. No such showing of suspicion of wrongdoing, however, is required under the FAA. The intelligence agencies can intercept all communications between U.S. persons and non-U.S. persons; the FAA makes no other limitations.

Under the *Liberty* guidelines, minimization procedures should be explicitly laid out in the statute so that the authorities cannot intrude into the private conversations among people in a way that is discriminatory or arbitrary. The FAA, however, fails to specify the details of the minimization procedures which the intelligence agencies are required to adopt. Lastly, because there are no guidelines on when recordings must be erased or destroyed, and there is nothing preventing the government from compiling all the intelligence data collected under this surveillance program into searchable

databases, the FAA would fail under the *Liberty* safeguard analysis.

CONCLUSION

Because terrorism is a global problem, all nations around the world are confronted with having to balance the privacy rights of their citizens versus the pressing need of all governments to secure the national defense of their country. In assessing the United States' current surveillance practices, it is beneficial to be aware of how other nations have struck the balance between individual liberty and national security, as that may impact one's conclusion of whether or not the FAA is reasonable. In the end, however, the question is ultimately one of Fourth Amendment constitutional analysis. Although the future of privacy rights in this country is not clear, there is good reason to believe that should the Supreme Court hear *Amnesty v. McConnell*, the Court will strike down the FAA as unconstitutional.