Saint Louis University Public Law Review

Volume 22 Number 1 *New Approaches to Ensuring the Legitimacy of Policy Conduct (Volume XXII, No.* 1)

Article 14

2003

Freedom of Liberty Takes on the Right to Privacy: An Analysis of Adams v. City of Battle Creek, The Circuit Split, and Possible Consequences of Anti-Terrorism Legislation

Michelle Schipke Silies

Follow this and additional works at: https://scholarship.law.slu.edu/plr

Part of the Law Commons

Recommended Citation

Silies, Michelle Schipke (2003) "Freedom of Liberty Takes on the Right to Privacy: An Analysis of Adams v. City of Battle Creek, The Circuit Split, and Possible Consequences of Anti-Terrorism Legislation," *Saint Louis University Public Law Review*: Vol. 22 : No. 1, Article 14. Available at: https://scholarship.law.slu.edu/plr/vol22/iss1/14

This Note is brought to you for free and open access by Scholarship Commons. It has been accepted for inclusion in Saint Louis University Public Law Review by an authorized editor of Scholarship Commons. For more information, please contact Susie Lee.

FREEDOM OF LIBERTY TAKES ON THE RIGHT TO PRIVACY: AN ANALYSIS OF ADAMS v. CITY OF BATTLE CREEK, THE CIRCUIT SPLIT, AND POSSIBLE CONSEQUENCES OF ANTI-TERRORISM LEGISLATION

I. INTRODUCTION

The events of September 11, 2001, permanently changed the lives of every American and placed the federal government—more now than ever before in our nation's history—in the "hot seat" for the responsibility of protecting its citizens from terrorism. Spurred by the nation's media, Americans wanted to know whether the attacks on the World Trade Center and the Pentagon resulted from failures of technology or overly restrictive laws, and if neither, whether the failures resulted from institutional problems in our nation's intelligence and law-enforcement agencies. Congress and President Bush's anti-terrorism legislation imposes a great number of changes in our national security policies and practices, including federal wiretapping regulations.¹ However, along with these heightened security measures also comes the responsibility of heightened civil liability for individual rights, in particular, the right to privacy.

In the wake of September 11, the country's attitude toward the appropriateness of widespread surveillance seems to have drastically changed.² On the belief that increased surveillance is necessary to prevent similar future tragedies, President George W. Bush and Congress introduced proposals for expanding the powers of federal agents in several important respects, including the authority to conduct electronic surveillance.³ The events of September 11 have also renewed a long-standing national debate about the proper balance

^{1.} Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [herinafter USA PATRIOT ACT].

^{2.} *Cf.* Neil Munro & Peter H. Stone, A Tougher Balancing Act, 33 NAT'L J. 2852 (2001) (noting how the terrorist attacks will likely lead to demands for increased law-enforcement capabilities, particularly in the area of surveillance, and stating that "[privacy] advocates now face a potentially insurmountable political problem: a wave of public disgust and fear that will likely help boost police budgets and surveillance authority nationwide"); David Barstow, *Envisioning an Expensive Future in the Brave New World of Fortress New York*, N.Y. TIMES, Sept. 16, 2001, at 16 (discussing how attitudes about security are likely to change).

^{3.} See Jonathan Krim, Anti-Terror Push Stirs Fears for Liberties: Rights Groups Unite To Seek Safeguards, WASH. POST, Sept. 18, 2001, at A17 (reporting on Attorney General John Ashcroft's introduction of a revised and expanded anti-terrorism legislative proposal).

SAINT LOUIS UNIVERSITY PUBLIC LAW REVIEW

[Vol. 22:207

between the government's powers to maintain order and national security and its citizens' Constitutional liberties.

These conflicting views of freedom of liberty verses an individual's right to privacy typify the debate over the proper balance between granting the government authority to maintain order in society and restraining the government from intruding on personal liberties.⁴ It is essential that our nation attempt to find and maintain a proper balance given the potential risks facing our society, increasingly sophisticated technologies, and our substantial and growing dependence on those sophisticated technologies. Although the new anti-terrorism measures are necessary and appropriate in light of the events of September 11, it is important to bear in mind that the federal government already possesses substantial power and technologies in those areas.

Underscoring this issue is the recent Second and Seventh Circuit Court split. The Sixth Circuit in Adams v. City of Battle Creek⁵ agreed with the Second Circuit and disagreed with the Seventh Circuit in holding that a government entity may be liable in a civil suit under the federal wiretap act, also known as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.6 With certain exceptions, the Electronic Communications Privacy Act criminalizes and creates civil liability for intentionally intercepting electronic communications without a judicial warrant.⁷ In Adams, through the use of a duplicate or "clone" pager and without a warrant, the police department tapped the plaintiff police officer's department-provided pager because the department erroneously thought the officer was assisting drug dealers.⁸ In granting summary judgment to defendants, the district court in Adams held that certain exceptions to the Electronic Communications Privacy Act applied.⁹ However, these exceptions—the business use and the law enforcement exceptions of the Act-required that the clone pager be used in the ordinary course of police business.¹⁰ Adams turns on what is meant by the Act's use of the phrase "in the ordinary course of business" to create these two exceptions to the prohibition against wiretapping.¹¹

^{4.} *See* United States v. United States District Court (Keith), 407 U.S. 297, 314-15 (1972) ("As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression.").

^{5.} Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001).

^{6.} Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522 (2001).

^{7.} Adams, 250 F.3d at 982.

^{8.} *Id*.

^{9.} *Id.* at 980.

^{10.} *Id.*

^{11.} Id. at 982.

209

2003] FREEDOM OF LIBERTY TAKES ON THE RIGHT TO PRIVACY

Section II of this comment will discuss and attempt to explain the case law history of wiretapping along with new developments in this area of law, including anti-terrorism legislation. Regrettably, the law surrounding the Fourth Amendment as applied to electronic surveillance has scarcely kept up with the today's technological advances. Section III of this comment will analyze the Sixth's Circuit's decision in *Adams*, the Second and Seventh Circuits' split and how those decisions may affect the federal government's liability for heightened wiretapping to prevent terrorism in the United States in light of the events of September 11. Specifically, Section III will analyze three of the five major issues in *Adams*: (1) The meaning of the phrase "other than" in the federal wiretapping act; (2) exceptions to liability; and (3) municipal liability under the privacy act.¹² *Adams'* issues of the Fourth Amendment and qualified immunity for Defendant Kruithoff are beyond the scope of this comment and will not be discussed.¹³

II. HISTORY AND BACKGROUND

A. Governing Law of Wiretapping

1. Case Law

In 1928, the U.S. Supreme Court decided *Olmstead v. United States.*¹⁴ This was its first ruling on the constitutionality of a modern surveillance technology, namely wiretapping.¹⁵ Several states, including Washington—where Mr. Olmstead and his co-conspirators were conducting an illegal liquor enterprise—had enacted laws to limit and control wiretapping.¹⁶ Federal agents installed wiretaps on eight of the suspects' phones and collected extensive evidence of a large conspiracy to violate the National Prohibition Act.¹⁷ The Court held that wiretapping did not violate the Fourth Amendment so long as there was no physical invasion of the target's premises,¹⁸ noting the Fourth Amendment's reference to "material things"¹⁹ and the significance of physical invasions in prior Fourth Amendment cases.²⁰

^{12.} Id. at 983-86.

^{13.} *Id.* at 986-87.

^{14.} Olmstead v. United States, 277 U.S. 438 (1928).

^{15.} *Id*.

^{16.} Id. at 479-80 & n.13 (Brandeis, J., dissenting) (listing state wiretap statutes).

^{17.} *Id.* at 471 (Brandeis, J., dissenting) (noting that the wiretaps spanned nearly five months and during that time the federal agents accumulated 775 pages of notes on conversations).

^{18.} Id. at 466.

^{19.} *Id.* at 464 ("The Amendment itself shows that the search is to be of material things - the person, the house, his papers or his effects.").

^{20.} Id. at 464-65.

In 1967 in *Berger v. New York*,²¹ the Court found that a New York eavesdropping statute that authorized electronic surveillance in certain circumstances failed to particularly describe the place to be searched and the persons or things to be seized, and that it therefore allowed electronic eavesdropping in a generalized and unconstitutional manner.²² Later that same year, the Court decided the dividing line case *Katz v. United States*,²³ which rejected trespass as the dispositive factor in warrantless electronic surveillance cases and which held that wiretapping was a search under the Fourth Amendment.²⁴ The Court stated that "the Fourth Amendment protects people, not places,"²⁵ and reasoned that a warrant was required before law-enforcement officers could wiretap telephone calls that Katz was making from a public pay phone.²⁶

These decisions explain one reason the courts have been reluctant to grant sweeping authority to law enforcement agencies for electronic surveillance— the recognition that such surveillance is quite intrusive on an individual's right to privacy. Moreover, the Supreme Court recognized the threat to liberty inherent in electronic surveillance in its decision in *Berger*.²⁷ The Court referred to electronic eavesdropping as a "dragnet," in that all conversations, even in conversations with persons not even suspected of a crime, would be swept in.²⁸

2. Title III and the Electronic Communications Privacy Act of 1986

In passing legislation governing wiretapping, Congress recognized electronic surveillance techniques are intrusive and can be easily abused. For over three decades, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (OCCSSA) has governed electronic surveillance for criminal investigations.²⁹ Although Title III generally prohibits wiretapping, it creates

^{21.} Berger v. New York, 388 U.S. 41 (1967).

^{22.} Id. at 58-60.

^{23.} Katz v. United States, 389 U.S. 347 (1967).

^{24.} The Court explained:

We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.

Id. at 353.

^{25.} Id. at 351.

^{26.} Id. at 353-357.

^{27.} Berger, 388 U.S. at 84.

^{28.} Id. at 65.

^{29. 18} U.S.C. §§2510-22 (2001).

211

2003] FREEDOM OF LIBERTY TAKES ON THE RIGHT TO PRIVACY

an exception under which law enforcement can legally intercept oral, electronic, and wire communications in certain limited situations and under strict constraints.³⁰ In enacting Title III, Congress expressly sought to accommodate both the need for effective law enforcement and the need to protect citizens' right to privacy.³¹ To keep the wiretap statute current, Congress has subsequently amended Title III several times, the most significant of which are the Electronic Communications Privacy Act of 1986 ("ECPA")³² and the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"),³³ making it illegal to intercept communications over cordless telephones.³⁴

Title III was enacted in response to the *Berger* and *Katz* line of cases and was an attempt to get a handle on the law of wiretapping.³⁵ Title III was later divided into three sections by the Electronic Communications Privacy Act of 1986 (ECPA).³⁶ The first section governs the interception of communications (Title I); the second governs stored communications (Title II); and the third governs pen registers (Title III).³⁷ Title I restricts the government's use of electronic surveillance to specific situations and expands the scope of protection beyond the Fourth Amendment requirements. For example, court orders for electronic surveillance must be granted only by certain officials, cannot be granted in situations where other means for obtaining the information have not been tried and requires probable cause and a specific

Id. at 211-12.

37. 18 U.S.C. §§2510-22, Titles I, II, and III.

^{30. 18} U.S.C. § 2517 (2001).

^{31.} *See* 801, 82 Stat. at 211. In enacting Title III, Congress made four findings, the fourth of which was:

To safeguard the privacy of innocent persons, the interception of wire or oral communications where none of the parties to the communication has consented to the interception should be allowed only when authorized by a court of competent jurisdiction and should remain under the control and supervision of the authorizing court. Interception of wire and oral communications should further be limited to certain major types of offenses and specific categories of crime with assurances that the interception is justified and that the information obtained thereby will not be misused.

^{32.} Pub. L. No. 99-508, 100 Stat. 1848 (1986).

^{33.} Pub. L. No. 103-414, 108 Stat. 4279 (1994).

^{34.} Pub. L. No. 103-414, 202, 108 Stat. 4279, 4290 (amending 18 U.S.C. §§ 2510, 2511 to include cordless telephones within Title III coverage).

^{35.} See, Daniel J. Solove, Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 S. CAL. L. REV. 1083-1167 at 1138.

^{36.} Amendment to Title III under the Electronic Communications Privacy Act: Wiretap Act, Electronic Communications Privacy Act, Title I, 18 U.S.C. §§ 2510-22 (2001); Stored Communications Act, Electronic Communications Privacy Act, Title II, 18 U.S.C. §§ 2701-11 (2000); Pen Register Act, Title III, 18 U.S.C. §§ 3121-27 (2000).

description of the place, time and type of communication to be intercepted.³⁸ Further, electronic surveillance is only permitted for certain crimes and not, for example, misdemeanors.³⁹ Because the information is stored by a third party, thereby reducing the expectation of privacy, Title II is much less restrictive.⁴⁰ Finally, Title III of the ECPA covers pen registers or trap and trace devices, which track the phone numbers dialed but not the conversations that took place.⁴¹ Previous case law provided that pen registers were not subject to Fourth Amendment protection because a person had no expectation of privacy as to the numbers.⁴² Title III gave very limited protection against pen registers by forcing the government to obtain a court order prior to use, although the order is granted on the mere requirement that the use is "relevant to an ongoing criminal investigation."⁴³

3. FISA: Wiretapping and Interception of Electronic Communications

As apart from domestic crime, the U.S. government needed measures to protect itself and its citizens from foreign intelligence and terrorism. Hence, Congress enacted the Foreign Intelligence Surveillance Act of 1978 ("FISA")⁴⁴ in response to remaining questions about whether surveillance by executive agencies in carrying out their national-defense function were covered by Title III.

FISA allows the government's executive branch to conduct wiretapping for national security purposes but still requires authorization to conduct such surveillance.⁴⁵ Requests for wiretaps are reviewed by a seven-member special court (the FISA court) under which the Attorney General must show probable cause for believing that the wiretap is for intelligence purposes.⁴⁶ No requirement for probable cause for suspecting the commission of a crime was required under FISA, however.⁴⁷ This made the standard for obtaining a

^{38.} Id.

^{39.} Id.

^{40.} See United States v. Kennedy, 81 F. Supp. 2d 1103, 1106 (D. Kan. 2000), in which an internet provider allowed the government access to a subscriber's computer, leading to the discovery of his possession of child pornography. The search was upheld due to the defendant knowingly revealing his IP address to the internet provider. *Id.* at 1110.

^{41. 18} U.S.C. §2510-22, Title III.

^{42.} See Smith v. Maryland, 442 U.S. 735 (1979).

^{43. 18} U.S.C. § 3121(a) (2000).

^{44.} The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C.S. §§ 1801-1863 (2000). [hereinafter FISA].

^{45.} *Id*.

^{46.} *Id*.

^{47.} *Id*.

warrant under FISA lower than obtaining a wiretap for law-enforcement purposes.⁴⁸

Along the same lines, the Supreme Court held in *United States v. United States District Court*⁴⁹ (commonly known as *Keith*) that the interposition of a judge was necessary for surveillance by executive-branch intelligence agencies for domestic national security.⁵⁰ This decision did not mandate the application of Title III procedures for such surveillance for domestic national security,⁵¹ and invited Congress to construct other protective procedures.⁵² Although the president's powers are at their greatest when acting for national security, in light of abuses by federal intelligence agencies, Congress requires the president to get a surveillance order to conduct a wiretap for national security purposes.⁵³ While the standard for getting a surveillance order to wiretap for intelligence purposes is lower than a surveillance order for law-enforcement purposes,⁵⁴ Congress has sought to require some level of accountability of intelligence agents.

In addition, as opposed to the requirements under other wire tap acts,⁵⁵ there is no notice requirement under FISA.⁵⁶ Surveillance under FISA can last from 90 days to a year. Targets of FISA surveillance may find it difficult to challenge the legality of the surveillance because the application for the surveillance is sealed and not available during discovery.⁵⁷ For all of these reasons, FISA surveillance is considerably friendlier to government than the surveillance under the ECPA.

To balance the potential for abuse,⁵⁸ Congress set forth several procedural safeguards. FISA requires probable cause for believing that a U.S. citizen was an agent of a foreign power—that is, one knowingly engaged in covert intelligence gathering activities, prior to surveillance.⁵⁹ By limiting the strong FISA provisions to this narrow purpose, Congress achieved a balance between

^{48.} Cf. Katz, 389 U.S. at 347.

^{49.} United States v. United States District Court (Keith), 407 U.S. 297 (1972).

^{50.} Id. at 323-24.

^{51.} *Id.* at 322 ("We do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case.").

^{52.} *Id.* ("Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.").

^{53.} FISA, supra note 44.

^{54.} Id.

^{55.} See infra notes 112-116 and accompanying text.

^{56.} FISA, supra note 44.

^{57.} Id.

^{58.} FISA of 1978 was enacted in the wake of the Watergate scandal, which eroded the trust of the American people in the executive branch.

^{59. 50} U.S.C. § 1801(b) (2000).

national security and individual rights.⁶⁰ Further, FISA limited electronic surveillance to situations where the "sole or main purpose" of the surveillance was to gather foreign intelligence information.⁶¹ Minimization procedures are also provided by FISA to reduce the probability that the information sought is necessary for the investigation.⁶²

Still, there exists the possibility that the government could attempt to find a way around these limitations by concealing a criminal investigation in the cloak of foreign intelligence. Courts reviewing evidence gathered using a FISA search repeatedly upheld the primary purpose requirement, although some courts refuse to draw a distinction between foreign intelligence crimes and ordinary criminal activities.⁶³ In response to these court decisions, in 1995 the Attorney General adopted Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations.⁶⁴ These procedures limited contact between the CIA, which in its charter is barred from engaging in internal security functions (domestic security),⁶⁵ and the Department of Justice (DOJ). This separation was an attempt to prevent the investigation from appearing or actually becoming a criminal investigation, by preventing the Criminal Division from "directing or controlling" the investigation.⁶⁶

4. Legislative Proposals After the Terrorist Attacks of September 11

Shortly after the attacks of September 11, there was a inundation of legislative measures aimed at combating terrorism.⁶⁷ The foremost issue Congress was concerned with was the lack of communication between the FBI and law enforcement agencies—due to the fact that it was collectively thought that the attacks could have been averted with appropriate collaboration. Alarmed by this haste and lack of thoughtful deliberation,⁶⁸ legislators and advocacy

68. Congress was pressured to act quickly on the bill submitted by Attorney General Ashcroft. *See* Krim, *supra* note 3 ("The White House is pushing for Capitol Hill to act by the end of the week, according to a congressional source.").

^{60.} Id.

^{61. 50} U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000).

^{62.} Id.

^{63.} See United States v. Sarkinssian, 841 F.2d 959 (9th Cir. 1988).

^{64. 1995} Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Couterintelligence Investigations.

^{65. 50} U.S.C. § 403-3(d)(1)(2000).

^{66.} Id.

^{67.} On September 13, the Senate attached an amendment, entitled the Combating Terrorism Act of 2001, to an appropriations bill for the Justice Department. *See* Senate Amendment 1562, 147 Cong. Rec. S9401 (daily ed. Sept. 13, 2001). Attorney General John Ashcroft introduced a more comprehensive legislative agenda, which included nearly identical provisions to Senate Amendment 1562, the Combating Terrorism Act. *See* Krim, *supra* note 3.

groups, both traditionally liberal and conservative,⁶⁹ challenged the wisdom, motives and the constitutionality of certain legislative provisions. Nevertheless, in less than two months, Congress enacted and President Bush signed into law the USA Patriot Act⁷⁰ with overwhelming support.⁷¹

The USA Patriot Act⁷² altered the administrative functioning of several other legislative acts, including OCCSSA and FISA. The most relevant changes include Title II, "Enhanced Surveillance Procedures."⁷³ This Title allows the sharing of evidence between law enforcement officers and the CIA and includes an expanded role for the Director of the CIA in FISA investigations.⁷⁴ The USA Patriot Act further limits judicial oversight of electronic surveillance, allowing roving wiretaps and warrants without particulars, including the name and place to be searched.⁷⁵ Most relevant to the FISA court authorization, however, was the change of the "sole or main purpose" language in FISA to "significant purpose,"⁷⁶ a move that lowers the burden for the government.

The USA Patriot Act also contains several provisions that significantly changed the law regarding the government's ability to conduct surveillance.⁷⁷ First, the USA Patriot Act makes terrorism a predicate act for which a wiretap under Title III of OSSCA can be authorized.⁷⁸ Second, it modified Title III, FISA and the federal statute related to pen registers (a close cousin to wiretaps and "bugs," which collects information about telephone calls placed to and from a target telephone, such as the telephone numbers dialed, the duration, and the time, for use in investigations and prosecutions of crimes) so that there would be explicit legal authorization to permit surveillance of e-mail and Internet communications.⁷⁹ Third, the Act authorizes the use of a "roving

- 73. USA Patriot Act, *supra* note 1, at § 203(b).
- 74. Id.
- 75. Id. at § 216(a).
- 76. Id. at § 218.
- 77. Krim, supra note 69.
- 78. USA PATRIOT ACT, *supra* note 1, at § 201.
- 79. USA PATRIOT ACT, supra note 1, at §§ 214, 216.

^{69.} See Krim, supra note 3 ("A coalition of public interest groups from across the political spectrum has formed to try to stop Congress and the Bush administration from rushing to enact counterterrorism measures before considering their effect on Americans' privacy and civil rights.").

^{70.} USA PATRIOT ACT, supra note 1.

^{71.} Jonathan Krim & Robert O'Harrow Jr., *Bush Signs into Law New Enforcement Era: U.S. Gets Broad Electronic Powers*, WASH. POST, Oct. 27, 2001, at A6.

^{72.} USA PATRIOT ACT, supra note 1.

wiretap" under FISA.⁸⁰ Fourth, the Act lowers the threshold for which surveillance pursuant to FISA is permitted,⁸¹ and expands the time-periods for which the Foreign Intelligence Surveillance Court can authorize surveillance in the United States of "an agent of foreign power."⁸² Fifth, the Act allows for so-called "sneak-and-peak warrants," which permit law-enforcement officers to delay notifying a target that a search or seizure has been conducted.⁸³ Sixth, the Act also lowers the firewalls that have been erected between law-enforcement and national-security agencies, by permitting greater sharing of information gained through surveillance.⁸⁴ Finally, the Act subjects several provisions to a four-year sunset.⁸⁵

In response to the passage of the Patriot Act, the Attorney General approved new Intelligence Sharing Procedures to replace the 1995 Procedures.⁸⁶ Under the new procedures, the "direction and control" test was abandoned in favor of a complete exchange of information between

Two circuit courts of appeal, the Second and the Ninth Circuits, have recognized a limited exception to this requirement [that a person be notified of a search]. When specifically authorized by the issuing judge or magistrate, the officers may delay providing notice of the search to avoid compromising an ongoing investigation or for some other good reason. However, this authority has been carefully circumscribed.

First, the Second and Ninth Circuit cases have dealt only with situations where the officers search a premises without seizing any tangible property. . . .

Second, the cases have required that the officers seeking the warrant must show good reason for the delay. Finally, while the courts have allowed notice of the search may be delayed, it must be provided within a reasonable period thereafter, which should generally be no more than seven days....

The bill prohibits the government from seizing any tangible property or any wire or electronic communication or stored electronic information unless it makes a showing of reasonable necessity for the seizure. . . . Second, the provision now requires that notice be given within a reasonable time of the execution of the warrant rather than giving a blanket authorization for up to a 90-day delay. What constitutes a reasonable time, of course, will depend upon the circumstances of the particular case. But I would expect courts to be guided by the teachings of the Second and the Ninth Circuits that, in the ordinary case, a reasonable time is no more than seven days.

^{80.} USA PATRIOT ACT, *supra* note 1, at § 206. The "roving wiretap" can now be obtained upon a showing that "the actions of the target of the application may have the effect of thwarting the identification of a specified person." *Id.*

^{81.} USA PATRIOT ACT, *supra* note 1, at § 218.

^{82.} USA PATRIOT ACT, supra note 1, at § 207.

^{83.} USA PATRIOT ACT, *supra* note 1, at § 213 (statement of Patrick Leahy). Senator Leahy explained sneak-and-peak warrants as follows:

Id. at S11002-03.

^{84.} USA PATRIOT ACT, *supra* note 1, at § 203(b)-(d).

^{85.} USA PATRIOT ACT, *supra* note 1, at § 224.

^{86.} Intelligence Sharing Procedures, March 6, 2002.

2003]

217

intelligence and law enforcement.⁸⁷ Further, the Procedures requested that the FISA court remove the minimization procedures in all cases.⁸⁸

III. ANALYSIS

A. Adams v. City of Battle Creek

Adams v. City of Battle Creek⁸⁹ was brought under the federal wiretapping act known as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522.⁹⁰ With certain exceptions, the federal wiretapping act criminalizes and creates civil liability for intentionally intercepting electronic communications without a judicial warrant.⁹¹ Adams raises the question of whether a police department may tap a police officer's pager without a warrant or notice to the officer.⁹²

David Adams, a City of Battle Creek police officer, brought suit against the city and a police department employee under § 1983 and the Electronic Communications Privacy Act, alleging that interception of pages he received over a department-issued pager through use of duplicate or "clone" pager violated his rights.⁹³ On cross-motions for summary judgment, the United States District Court for the Western District of Michigan granted summary judgment to defendants; Adams appealed.⁹⁴ The Court of Appeals, held that: (1) warrantless interception of pages was not made in ordinary course of police department's business, and thus did not come within exception to Act's prohibition on interception of electronic communications; (2) governmental entities may be held liable for violations of Act; (3) the court would decline to reach constitutional issues raised; and (4) factual issues as to whether city could be held liable, and whether department employee was protected by qualified immunity, precluded summary judgment.⁹⁵ The case was affirmed in part, reversed in part, and remanded.⁹⁶

In *Adams*, it is both clear and accepted that the definition of "intercept" in the Act includes pagers within the language "acquisition of the contents of any . . . electronic . . . device."⁹⁷ The statutes' definition section for "electronic

- 87. Id.
- 88. Id.
- 89. 250 F.3d 980.
- 90. Id. at 982.
- 91. Id.
- 92. Id.
- 93. Id. at 980.
- 94. Id.
- 95. Id.
- 96. Id.
- 97. Id. at 982.

SAINT LOUIS UNIVERSITY PUBLIC LAW REVIEW

[Vol. 22:207

device" creates two "in-the-ordinary-course-of-business" exceptions to wiretap liability.⁹⁸ The scope and meaning of these two exceptions are in need of interpretation, because the two exceptions are not exactly clear.⁹⁹

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication *other than* -

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business *and being used by the subscriber or user in the ordinary course of its business* or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire of electronic communication service in the ordinary course of business, or by an investigative or law enforcement officer in the ordinary course of his duties.¹⁰⁰

The first problem the Court found is what the underlined phrase "other than" (normally an adverbial phrase) is supposed to modify.¹⁰¹ The Court questioned whether it modifies the immediately preceding action "to intercept [an]... electronic device," or whether it acts as an adjective, modifying "device or apparatus" or does it modify some other action or thought not expressed in clear language.¹⁰² The second problem the Court found is whether the use of "in-the-ordinary-course-of-business" language, as an exception, implies, and therefore means, that the tapping of the communication is so routine, customary or well accepted that the parties to the tapped communication would, should or did know of the tap.¹⁰³ The court in *Adams* dealt with these two issues of interpretation as set out below.

1. The Meaning of the Phrase "Other Than"

The Court found that there is no discussion in the case law of what the phrase "other than" in the statutory definition of "electronic, mechanical or other device" is to modify.¹⁰⁴ The *Adams* court stated that its dictionary label as an adverbial phrase indicates that it is to modify the immediately preceding verb phrase "to intercept a wire, oral, or electronic communication," and found that this does not make sense when read with the language that follows it.¹⁰⁵

^{98.} Id.

^{99.} Id.

^{100. 8} U.S.C. § 2510(5) (2001) (emphasis added).

^{101.} Adams, 250 F.3d at 983.

^{102.} Id.

^{103.} *Id*.

^{104.} Id.

^{105.} Id.

219

2003] FREEDOM OF LIBERTY TAKES ON THE RIGHT TO PRIVACY

The Court reasoned that if "other than" modifies "used to intercept... electronic communication, "the scope of the "other than" exception would be as broad as the statute itself.¹⁰⁶ Therefore, this means that "other than" must modify the nouns "device or apparatus."¹⁰⁷ The language immediately following "other than" is "any telephone or telegraph, or any component thereof," all of which are also nouns.¹⁰⁸ The Court reasoned that a better word choice than the "other than" phrase probably would have been "excluding" because subparts (a) and (b) to § 2510 (5) are exclusions to the main definition.¹⁰⁹ The Court noted that the cases discussing these exceptions apply "other than" this way, and it is the only way that makes sense.¹¹⁰

2. In the Ordinary Course Exceptions to Liability

The Court in Adams concluded that the exceptions to liability do not apply to this case, and held that both the "ordinary course of business" exception, or "business use" exception as it is also called, as well as the law enforcement exception, require that the interception of a communication be undertaken by employers or law enforcement agencies in the ordinary course of their businesses using equipment provided by a communications carrier as part of the communications network.¹¹¹ The Court stated that for this exception to apply, a court must find, first, that the equipment used to make the interception be "furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business ... § 2510(5)(a)(i)."¹¹² Although the plaintiff raised the issue of whether a clone pager fits within the definition prescribed in the exception, the Court found it clear that the clone pager, a piece of electronic communication equipment, was provided to the City by MobileComm, a Bell South company, in the ordinary course of its business as a provider of wire and electronic communication services.¹¹³ The Court found, as did the district court, that the first part of the exception is met.¹¹⁴

The Court held that the second part of the exception requires that the clone pager be used in "the ordinary course" of the police department's business.¹¹⁵

- 106. *Id*.
- 107. *Id*.
- 108. Id.
- 109. Id.
- 110. *Id*.
- 111. Id.
- 112. Id.

- 114. Id. at 984.
- 115. Id.

^{113.} Id. at 983-84.

"Ordinary course of business" is not defined in the statute, but generally requires that the use be (1) for a legitimate business purpose, (2) routine and (3) with notice.¹¹⁶ The Court noted there is some disagreement in the case law about whether "covert" monitoring can ever be in the "ordinary course of business."¹¹⁷ Although the Court did not find that the statute requires actual consent for the exception to apply, the Court held that monitoring in the ordinary course of business requires notice to the person or persons being monitored.¹¹⁸ The Court held that, because it is undisputed that plaintiff was not given any notice that his pager was being monitored, the exceptions cannot apply.¹¹⁹

Most courts interpreting these exceptions have held that advance notice in some form is necessary.¹²⁰ "What is ordinary is apt to be known; it imports implicit notice."¹²¹ In *Amati v. City of Woodstock*,¹²² employees and former employees of a police department, along with friends and family members, brought an action against the city, the former police chief, and other members of the police department under the federal electronic-eavesdropping statute, based on alleged taping of plaintiffs' personal telephone calls.¹²³ The court held that the recording of all calls to and from a police department was routine police practice and, thus, took place in the ordinary course of a law enforcement officer's duties for purpose of the exception to liability under the federal electronic-eavesdropping statute, *regardless of whether police employees were aware that particular line was being taped* (emphasis added).¹²⁴

In *Bohach v. City of Reno*,¹²⁵ claiming violations of the Fourth Amendment and the wiretap statutes, police officers sought to halt an investigation into their alleged misuse of the department's computerized paging system. The police department was retrieving stored messages generated by their pagers.¹²⁶ The court held that the officers had no reasonable expectation of privacy when the police department warned pager users in advance that their messages would be logged on the network.¹²⁷ The court noted that the police officers did not

220

120. See id.

120 S. Ct. 445.

123. Id.

124. Id. at 955.

125. Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

126. Id. at 1233.

127. Id. at 1235.

^{116.} *Id*.

^{117.} Id.

^{118.} Id.

^{119.} Id.

^{121.} Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir.), cert. denied, 528 U.S. 985,

^{122.} Amati v. City of Woodstock, 176 F.3d 952.

have reasonable expectation of privacy in their use of the computerized paging system because all messages were recorded and stored.¹²⁸ Storage of the messages was not due to anyone "tapping" the system but was simply an integral part of the technology, which stored messages in central computer until they were retrieved by, or sent to, the intended recipient.¹²⁹ Transmission from a user's keyboard to a computer was essentially electronic mail.¹³⁰ The police chief had notified all users that their messages would be "logged on the network," that certain types of messages were banned from the system, and that police stations often record all outgoing and incoming telephone calls.¹³¹

In *Sanders v. Robert Bosch Corp.*,¹³² the Fourth Circuit held that recording all telephone conversations on certain lines after bomb threats were received by the company was not in the ordinary course of business where the employees did not receive notice of the recording.¹³³ The court further held that there was no unlawful "interception" of a security officer's conversations during the period after the corporation that retained the security firm turned off the voice logger on telephone lines with extensions in the security office, even though, due to a design defect, a handset microphone remained able to pick up ambient noise in the guards' office and transmit it to the corporation's security control room where employees did not receive notice of the recording.¹³⁴

The Sixth Circuit in *Adams v. City of Battle Creek* agreed with the Second Circuit and disagreed with the Seventh Circuit in holding that a government entity may be liable in a civil suit under 18 U.S.C. §§ 2510-2522. The defendants in *Adams* did not routinely monitor officers' pagers nor give notice to officers that random monitoring of their department-issued pagers was possible.¹³⁵ The Court disagreed with defendants to the extent that they contend that Adams impliedly consented to the interception of his pages by the clone pager simply because he accepted and used a department-issued pager.¹³⁶ The Court stated that the general policy of the department that department-issued equipment, which includes the pager, was not to be "converted to surreptitious interception of their messages by clone pagers.¹³⁷ The Court went on to state that the so-called policy prohibiting personal use cannot form an

^{128.} Id. at 1234-35.

^{129.} Id.

^{130.} Id.

^{131.} Id.

^{132.} Sanders v. Robert Bosch Corp., 38 F.3d 736 (4th Cir. 1994).

^{133.} Id. at 739.

^{134.} Id. at 742.

^{135.} Adams, 250 F.3d at 984.

^{136.} *Id*.

^{137.} Id.

SAINT LOUIS UNIVERSITY PUBLIC LAW REVIEW

[Vol. 22:207

after-the-fact justification for intercepting plaintiff's pager where the policy had not been enforced and the department conceded it was aware that pagers were used by many members of the force for personal use.¹³⁸

The Court did not find any need under the facts presented in this case to analyze the "business use" and "law enforcement" exceptions separately.¹³⁹ The Court noted that Congress most likely carved out an exception for law enforcement officials to make clear that the routine and almost universal recording of phone lines by police departments and prisons, as well as other law enforcement institutions, is exempt from the statute.¹⁴⁰ Such a system routinely and indiscriminately records all phone activity in and out of the police department.¹⁴¹ This practice is well known in the industry and in the general public, and the courts have ruled that even prisoners are entitled to some form of notice that such conversations may be monitored or recorded.¹⁴²

This point is illustrated in *United States v. Paul.*¹⁴³ In *Paul*, defendants were convicted in the United States District Court for the Eastern District of Kentucky, impart based on evidence of their phone conversations, under a statute making it unlawful for anyone to introduce, on the grounds of a federal prison, anything contrary to the rule of the Attorney General, and they appealed.¹⁴⁴ The Court of Appeals held that where monitoring of telephone at prison took place pursuant to policy statement issued by Federal Bureau of Prisons as well as local prison rules, telephone rules were posted, and prison inmates had reasonable notice that monitoring of their conversations might occur, monitoring took place within ordinary course of correctional officer's duties and was permissible under exception to Title III, permitting interception of communications over equipment used by an investigative or law enforcement officer in the ordinary course of his duties and therefore trial court did not err in refusing to suppress testimony regarding such monitored telephone conversations.¹⁴⁵

Also illustrating this point is *United States v. Daniels*,¹⁴⁶ wherein the court held that the provision of the criminal code allowing wiretapping by an investigative or law enforcement officer in the ordinary course of his duties

^{138.} Id.

^{139.} Id.

^{140.} Id. (citing First v. Stark Cnty. Bd. Of Comm'rs, 2000 WL 1478389 (6th Cir. Oct. 4, 2000)).

^{141.} Adams, 250 F.3d at 984.

^{142.} *Id.* (citing United States v. Paul, 614 F.2d 115 (6th Cir. 1980); United States v. Daniels, 902 F.2d 1238, 1245 (7th Cir. 1990); United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)).

^{143.} United States v. Paul, 614 F.2d (6th Cir. 1980).

^{144.} Id. at 115-16.

^{145.} Id. at 116-17.

^{146.} United States v. Daniels, 902 F.2d 1238 (7th Cir. 1990).

allowed the Federal Bureau of Investigation to record an inmate's telephone calls from jail, during which the inmate conducted an illegal enterprise. Thus, evidence obtained by recording did not have to be suppressed in criminal trial.¹⁴⁷ Further, in *United States v. Amen*,¹⁴⁸ the court held that (1) Title III of the Omnibus Crime Control and Safe Streets Act dealing with wiretapping applies to prison monitoring; (2) inmates impliedly consented to interception of their telephone calls by using prison telephones when they were on notice of the prison's interception policy from at least four sources; (3) taping of telephone conversations made by prison inmates did not violate the Fourth Amendment; (4) prison inmates have no reasonable expectation of privacy; and (5) in the prison context, the reasonableness of this search is directly related to legitimate concerns for institutional security.¹⁴⁹

3. Municipal Liability Under the Privacy Act

In *Adams*, the plaintiff sought to hold both the City and a police department employee liable under the wiretapping act.¹⁵⁰ The defendants raised the question of whether the City is a "person" for purposes of the Act.¹⁵¹ The Court answered that question by noting that the statute defines "person" as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust or corporation."¹⁵²

The *Adams* court noted that the provision of the Act providing for civil liability, § 2520,¹⁵³ was amended in 1987 and made part of the 1986 Privacy Act.¹⁵⁴ The amendment added the words "or entity" to those who may be held liable under the Act.¹⁵⁵ The addition of the words "entity" can only mean a governmental entity because prior to the 1986 amendments, the definition of "person" already included business entities.¹⁵⁶ In order for the term not to be redundant, the term "entity" necessarily means governmental entities.¹⁵⁷ The

^{147.} *Id.* at 1245.

^{148.} United States v. Amen, 831 F.2d 373 (2d Cir. 1987).

^{149.} Id. at 378-80.

^{150.} Adams, 250 F.3d at 984.

^{151.} Id. at 985.

^{152.} Id.

^{153.} Id.

^{154. 18} U.S.C. § 2520 (2001) provides:

Except as provided in § 2511(2)(ii), any person whose wire, oral or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

^{155.} Adams, 250 F.3d at 985.

^{156.} Id.

^{157.} Id.

Court noted in support of this view that the amendment added the same language to the civil liability provision for interception of stored wire and electronic communications under 18 U.S.C. § 2707(a).¹⁵⁸ The Court noted that the Senate Committee Report summarizing § 2707, the parallel section for liability for intercepting stored communications, specifically states that the word "entity" includes governmental entities.¹⁵⁹

The Court based its decision on the amendments to the statute and the legislative history behind them, as well as the case law considering the issue, in holding that governmental entities may be liable under 18 U.S.C. § 2520.¹⁶⁰ The Court, in finding that a municipality may be liable under the Act, concluded that questions of material fact still remain as to who was involved in authorizing the interception and how it arose.¹⁶¹ The Court held that summary judgment was not appropriate on this issue at that time because the facts were undeveloped, and remanded the case to the district court for further development of this issue.¹⁶²

B. Sixth Circuit's Dissent in Adams

Circuit Judge Krupansky concurred in part and dissented in part.¹⁶³ The panel majority reversed the district court's grant of summary judgment to the defendant-appellees, finding that the electronic monitoring at issue in this case did not fall within one of the statutory exclusions provided by the federal wiretapping laws.¹⁶⁴ In so doing, Judge Krupansky noted, the panel majority disregarded the plain language of the controlling statute by imputing a notice requirement into the ordinary course of business and law enforcement tests of the federal wiretapping laws.¹⁶⁵

Circuit Judge Krupansky noted that David Adams had served as a law enforcement officer¹⁶⁶ for the City of Battle Creek Police Department since 1986.¹⁶⁷ In conjunction with his position as a law enforcement officer, Adams was assigned an alphanumeric pager.¹⁶⁸ The police department had given Adams a copy of departmental policy which indicated "Department issued

^{158.} Id.

^{159.} Id.

^{160.} S. Rep. No. 541, 99th Cong., 2d Sess. 43 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3597.

^{161.} Adams, 250 F.3d at 985.

^{162.} Id. at 985-86.

^{163.} Id. at 987.

^{164.} Id.

^{165.} Id.

^{166.} Id. David Adams served as a patrolman until 1993 when promoted to the position of detective.

^{167.} Id.

^{168.} *Id*.

equipment, supplies and uniforms, will at no time be converted [to] personal use."¹⁶⁹ The police department had notified Adams that "[it was] the policy of the Police Department to perform regular audits and inspections of all department issues equipment.¹⁷⁰ These inspections ensure proper maintenance and use of all department equipment and supplies."¹⁷¹ Numerous allegations of complicity in drug activity have marked his tenure: (1) in 1989, his patrol partner was charged with drug trafficking; (2) a number of informants alleged that Adams had protected drug dealers; and (3) Adams had appeared to maintain a close friendship with a local drug dealer.¹⁷² However, investigators had failed to surface substantial evidence of wrongdoing by Adams.¹⁷³

Circuit Judge Krupansky dissented because he was persuaded that the officers of the City of Battle Creek Police Department monitored David Adams' use of his alphanumeric pager in the ordinary course of its business according to the exception in 18 U.S.C. § 2510(5)(a)(i), and in the ordinary course of exercising their law enforcement duties according to the exception in 18 U.S.C. § 2510(5)(a)(i).

C. The Second Circuit's Analysis

Most courts addressing the issue have held that the 1986 amendments indicate that a governmental entity may be liable in a civil suit under the Act.¹⁷⁵ In *Organizacion JD Ltda. v. United States Department of Justice,* bank account holders victimized by government seizure of numerous electronic fund transfers brought suit against the government and various banks.¹⁷⁶ The United States District Court for the Eastern District of New York dismissed the complaint in its entirety.¹⁷⁷ The Court of Appeals held that: (1) government entities could be liable for violating the statute regulating access to stored electronic information, and (2) remand would be required for additional fact determinations as to whether government had been liable in present case.¹⁷⁸

The Court in *Organizacion* stated that the government did not violate Electronic Communications Privacy Act by seizing electronic wire transfers of

^{169.} *Id*.

^{170.} *Id*.

^{171.} Id.

^{172.} Id.

^{173.} Id.

^{174.} Id.

^{175. 18} U.S.C. § 2510(6)(2001); *see also* Organizacion JD Ltda. v. United States Dep't of Justice, 18 F.3d 91, 94-95 (2d Cir. 1994); Conner v. Tate, 130 F. Supp. 2d 1370 (N.D. Ga. 2001); PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 822-23 (D.N.J. 1993).

^{176.} Organizacion JD Ltda. v. United States Dept. of Justice, 18 F.3d 91 (2d Cir. 1994).

^{177.} Id. at 93.

^{178.} Id. at 93-94.

funds claimed to have been obtained from illegal drug transactions and held that no required "interception" had occurred because no "device" as defined under Act had been used.¹⁷⁹ The court also held that government entities are subject to liability under the statute regulating access to certain stored electronic records.¹⁸⁰

In *Conner v. Tate*,¹⁸¹ a citizen brought an action against a county, county officers and woman who allegedly unlawfully accessed and taped private telephone and voice mail communications between the citizen and the woman's former husband, seeking damages for alleged violations of federal and state wiretap statutes and Electronic Communications Privacy Act.¹⁸² The county moved to dismiss, and county officers moved for partial judgment on the pleadings.¹⁸³ The district court held that governmental entities are amenable to suit under the civil liability provisions of federal wiretap statutes and Electronic Communications Privacy Act authorizing civil damages for unlawful interception, disclosure or use of wire, oral or electronic communications.¹⁸⁴

The court held that as defined in federal wiretap statutes, the term "person" does not include governmental agencies, and therefore government entity cannot be prosecuted criminally for violation of wiretap statutes and that the statutory language is the starting point for interpreting the meaning of a statute.¹⁸⁵ If the statutory language being interpreted is ambiguous, the court may look to the legislative history and the overall statutory scheme.¹⁸⁶

The court went on to state that a county could be held civilly liable for violating the Electronic Communications Privacy Act.¹⁸⁷ The court held that the complaint failed to state a civil damages claim against the county for violating the Electronic Communications Privacy Act, given that the complaint did not allege that the county accessed the electronic communication service illegally, and allegations that a third party somehow obtained capability to access and record messages from voice mail systems and pager memories of the plaintiff and the third-party's husband did not permit inference that access was acquired with assistance of county police officers to whom recordings were later allegedly disclosed.¹⁸⁸

- 181. Conner v. Tate, 130 F. Supp. 3d 1370 (N.D. Ga. 2001).
- 182. Id. at 1373.
- 183. Id.
- 184. Id. at 1375.
- 185. Id. at 1374-75.
- 186. Id. at 1375.
- 187. Id.
- 188. Id.

^{179.} Id. at 94.

^{180.} Id. at 94-95.

227

2003] FREEDOM OF LIBERTY TAKES ON THE RIGHT TO PRIVACY

In *PBA Local No. 38 v. Woodbridge Police Department*,¹⁸⁹ the police officers union and individual officers sued the township, township police department, former and current police directors, former mayor and the telephone company alleging that electronic listening and taping devices were covertly placed in certain areas of police headquarters and on building phone lines resulting in unlawful interception of police officers' private conversations in violation of United States Constitution, New Jersey and Federal Wiretap Acts, and New Jersey common law.¹⁹⁰ On defendants' motions for summary judgment, the district court held that: (1) the police officers did not have reasonable expectation of privacy in conversations which took place over "beeped" telephone lines; (2) the police officers could not recover damages for humiliation, mental pain and anguish under New Jersey Tort Claims Act; (3) the union had no standing to bring claim; and (4) the police director was a "policy-making official" for purposes of municipal liability under § 1983.¹⁹¹

The district court held that telephone conversations which were recorded covertly in police headquarters were "wire communications," within the meaning of both the Federal Wiretap Act and the New Jersey Wiretap Act, and thus, the "reasonable expectation of privacy" standard did not govern claims; wire communications, unlike oral communications, were generally protected regardless of whether the person making or receiving such communications had an expectation of privacy.¹⁹² The court stated that the reasonable expectation of privacy standard of Katz¹⁹³ was highly relevant to claimed interceptions of the police officers' oral conversations by means of surreptitious recording in police headquarters in violation of both Federal and New Jersey Wiretap Acts.¹⁹⁴ "Person," in the definitional section of the federal wiretap statute, includes government employees but does not include governmental bodies themselves.¹⁹⁵ "Entity," within the meaning of the federal wiretap statute authorizing recovery from a person or entity that violates statute, refers to governmental entities; thus, governmental entities such as the township and police department were subject to liability under the Federal Wiretap Act.¹⁹⁶ "Person," within the meaning of the New Jersey Wiretap Act, does not include governmental bodies; thus, the township and police department could not be subject to liability under the New Jersey Wiretap

^{189.} PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808 (D.N.J. 1993).

^{190.} Id. at 814.

^{191.} Id. at 819-24.

^{192.} Id. at 819.

^{193.} Katz, 389 U.S. 347 (1967).

^{194.} PBA Local No. 38, 832 F. Supp. at 819.

^{195.} Id. at 822-23.

^{196.} Id. at 823.

SAINT LOUIS UNIVERSITY PUBLIC LAW REVIEW

Act.¹⁹⁷ Lastly, the court stated that in determining what construction to give to the New Jersey Wiretap Act, the court must weigh the fact that the Act was closely modeled after and made to substantially parallel the Federal Wiretap Act.¹⁹⁸

D. The Seventh Circuit's Analysis

228

Only the Seventh Circuit has ruled to the contrary, holding that a governmental entity may not be found liable in a civil suit under the Electronic Communications Privacy Act.¹⁹⁹ In *Amati v. City of Woodstock*,²⁰⁰ the court based its hasty decision to exempt governmental entities from liability under the Act solely on the plain language of the definition of "person" in the statute, which does not expressly include governmental entities.²⁰¹ The court did not deal with the meaning of the word "entity."²⁰² Finding no ambiguity, the court refused to look to the legislative history.²⁰³ However, the court in Adams looked to the legislative history in order to give meaning to the word "entity," which was added to the definition in 1987.²⁰⁴

The *Amati* court specifically held the following: (1) Exception to liability under federal electronic-eavesdropping statute that exists for eavesdropping by an investigative or law enforcement officer in the ordinary course of his duties is not limited to situations in which express notice is given to people whose conversations are being listened to;²⁰⁵ (2) for purpose of the exception to liability under federal electronic-eavesdropping statute that exists for eavesdropping by an investigative or law enforcement officer in the ordinary course of his duties, the term "ordinary" is properly interpreted to refer to routine noninvestigative recording of telephone conversations, not to use of wiretapping that occurs in furtherance of an investigation;²⁰⁶ (3) recording of all calls to and from the police department was routine police practice and thus took place in the ordinary course of a law enforcement officer's duties for the purpose of exception to liability under the federal electronic-eavesdropping statute, regardless of whether police employees were aware that particular line was being taped;²⁰⁷ (4) the federal electronic-eavesdropping statute does not

^{197.} Id. at 823-24.

^{198.} Id. at 824.

^{199.} Adams, 250 F.3d at 985.

^{200.} Id. (citing Amati, 176 F.3d at 956); see supra notes 121 and 122 and accompanying text.

^{201.} Adams, 350 F.3d at 985.

^{202.} Id.

^{203.} Id.

^{204.} Id.

^{205.} Amati, 176 F.3d at 955.

^{206.} Id.

^{207.} Id.

forbid all nonconsensual electronic eavesdropping, but it does require a warrant for electronic eavesdropping that is not within one of the exclusions;²⁰⁸ and (5) the federal electronic-eavesdropping statute does not allow for suits against municipalities.²⁰⁹

E. Author's Analysis

The Electronic Communications Privacy Act seeks to balance citizens' privacy rights and law enforcement needs while keeping in mind the protections of the Fourth Amendment against unreasonable search and seizure.²¹⁰ Congress has made the Act the primary means by which to address violations of privacy interests in the communications field.²¹¹ Bearing this in mind, the Electronic Communications Privacy Act and the *Adams*, Second Circuit and Seventh Circuit's decisions may have grayed the lines defining this balance—especially in light of the consequences of Congress and President Bush's new anti-terrorism legislation.

The Sixth Circuit in Adams correctly agreed with the Second Circuit and correctly disagreed with the Seventh Circuit in holding that a government entity may be liable in a civil suit under the Electronic Communications Privacy Act. The Court properly found that Adams turns on what is meant when the Act uses the phrase "in the ordinary course of business" to create two exceptions to the prohibition against wiretapping.²¹² The Court's reasoning that the statutes' definition section for "electronic device" creates two "in-theordinary-course-of-business" exceptions to wiretap liability²¹³ was correct. In finding that the exceptions do not apply to this case, the court correctly held that both the "ordinary course of business" exception and the law enforcement exception require that the interception of a communication be undertaken by employers or law enforcement agencies in the ordinary course of their businesses using equipment provided by a communications carrier as part of the communications network.²¹⁴ The Court relied on the fact that "ordinary course of business" is not defined in the statute, but generally requires that the use be (1) for a legitimate business purpose, (2) routine, and (3) with notice.²¹⁵

Adams' majority correctly reversed the district court's grant of summary judgment to the defendant-appellees, finding that the electronic monitoring at issue in this case did not fall within one of the statutory exclusions provided by

^{208.} Id.

^{209.} Id. at 956.

^{210.} Adams, 350 F.3d at 986.

^{211.} Id. at 986.

^{212.} Id.

^{213.} Id. at 982.

^{214.} Id.

^{215.} Id. at 983.

the federal wiretapping laws.²¹⁶ In so doing, the panel majority disregarded the plain language of the controlling statute by imputing a notice requirement into the ordinary course of business and law enforcement tests of the federal wiretapping laws.²¹⁷

Circuit Judge Krupansky dissent is not persuasive in that he argued that he was convinced that the officers of the City of Battle Creek Police Department monitored David Adams' use of his alphanumeric pager in the ordinary course of its business and in the ordinary course of exercising their law enforcement duties.²¹⁸

The majority of the courts addressing this issue in the Second Circuit have correctly held that the 1986 amendments indicate that a governmental entity may be liable in a civil suit under the Act.²¹⁹ Organizacion JD Ltda. v. United States Department of Justice²²⁰ held government entities could be liable for violating the statute regulating access to stored electronic information.²²¹ In Conner v. Tate,²²² the district court held that governmental entities are amenable to suit under the civil liability provisions of federal wiretap statutes and Electronic Communications Privacy Act authorizing civil damages for unlawful interception, disclosure or use of wire, oral or electronic communications.²²³ The court held that as defined in federal wiretap statutes the term "person" does not include governmental agencies, and therefore a government entity cannot be prosecuted criminally for violation of wiretap statutes.²²⁴ Conner held that a court may look to the legislative history and the overall statutory scheme if the statutory language being interpreted is ambiguous.²²⁵ In PBA Local No. 38 v. Woodbridge Police Department,²²⁶ held that "entity," within the meaning of the federal wiretap statute authorizing recovery from a person or entity that violates the statute, refers to governmental entities; thus, governmental entities such as a township and a police department were subject to liability under the Federal Wiretap Act.²²⁷

^{216.} Id. at 984.

^{217.} Id. at 987.

^{218.} Id.

^{219.} See Organizacion JD Ltda. v. United States Dep't of Justice, 18 F.3d 91, 94-95 (2d Cir. 1994); Conner v. Tate, 130 F. Supp. 2d 1370 (N.D. Ga. 2001); PBA Local No. 38 v. Woodbridge Police Dep't, 832 F. Supp. 808, 822-23 (D.N.J. 1993).

^{220.} Organizacion JD Ltda. v. United States Dep't of Justice, 18 F.3d 91 (2d Cir. 1994).

^{221.} Id. at 94-95.

^{222.} Conner v. Tate, 130 F. Supp. 3d 1370 (N.D. Ga. 2001).

^{223.} Id. at 1375.

^{224.} Id. at 1374-75.

^{225.} Id. at 1375.

^{226.} PBA Local No. 38, 832 F. Supp. at 814.

^{227.} Id. at 823.

Only the Seventh Circuit has ruled to the contrary in that it indicates that a governmental entity may not be held liable in a civil suit under the Electronic Communications Privacy Act.²²⁸ In *Amati v. City of Woodstock*,²²⁹ the court based its *hasty* decision to exempt governmental entities from liability under the Act solely on the plain language of the definition of "person" in the statute, which does not expressly include governmental entities.²³⁰ The court did not deal with the meaning of the word "entity."²³¹ Finding no ambiguity, the court incorrectly refused to look to the legislative history.²³² Is this to say the Seventh Circuit believes the government is above the law?

In opposition to *Amiti*, the court in Adams looked to the legislative history in order to give meaning to the word "entity," which was added to the definition in 1987.²³³ The Adams court noted that the provision of the Act providing for civil liability, § 2520,²³⁴ was amended in 1987 and made part of the 1986 Privacy Act.²³⁵ The amendment added the words "or entity" to those who may be held liable under the Act.²³⁶ The addition of the words "entity" can only mean a governmental entity because prior to the 1986 amendments, the definition of "person" already included business entities.²³⁷ In order for the term not to be redundant, the term "entity" necessarily means governmental entities.²³⁸ The Court correctly noted in support of this view that the amendment added the same language to the civil liability provision for interception of stored wire and electronic communications under 18 U.S.C. § 2707(a).²³⁹ The Court relied on the Senate Committee Report summarizing § 2707, the parallel section for liability for intercepting stored communications, which specifically states that the word "entity" includes governmental entities.240

F. Consequences of Anti-terrorism Legislation on Case Law

On November 18, 2002, the United States Foreign Intelligence Surveillance Court of Review reversed a Foreign Intelligence Surveillance

231. Id.

232. Id.

233. Id.

- 234. 18 U.S.C. § 2520 (2001).
- 235. Adams, 250 F.3d at 985.
- 236. Id.
- 237. Id.
- 238. Id.
- 239. Id.

3597.

^{228.} Adams, 250 F.3d at 985.

^{229. 176} F.3d 952.

^{230.} Adams, 350 F.3d at 985.

^{240.} S. Rep. No. 541, 99th Cong., 2d Sess. 43 (1986), reprinted in 1986 U.S.C.C.A.N. 3555,

Court decision²⁴¹ involving the application of Foreign Intelligence Surveillance Act (FISA).²⁴² The government, as the sole litigant, appealed a decision by the Foreign Intelligence Surveillance Court (the FISA court) that set limitations on orders authorizing electronic surveillance of an "agent of a foreign power."²⁴³ The FISA court's goal was to ensure that law enforcement officials do not use the electronic surveillance provisions of FISA for the unlawful purpose of furthering a criminal investigation, rather than for the intended purpose of protecting against foreign intelligence.²⁴⁴ In reversing the FISA court's decision, however, the Review Court found that the foreign intelligence element need not be the "primary purpose" for the search, but rather could be a mere "measurable purpose" of the search.²⁴⁵ The court reached its conclusion based on the language in FISA as passed by Congress in 1978,²⁴⁶ prior to the amendment by the USA Patriot Act of 2001.²⁴⁷ This conclusion reverses years of court decisions, is in conflict with the Fourth Amendment, and opens the door to abuse of FISA's authority.

The restriction of "primary purpose" prevents abuses of FISA and gives the federal government a guide for selecting targets for wiretaps. This newfound absence of such restrictions invites abuse. For example, wiretapping targets could easily become politically motivated. Although it is understandable in the wake of September 11, 2001, to want to grant as much discretion as possible to the government to prevent future terrorism attacks, the desire for safety from outside entities must be tempered with a desire for safety from governmental abuses of civil liberties.

IV. CONCLUSION

In concluding that government entities may be held liable in a civil suit under the Electronic Communications Privacy Act, the court in *Adams* delved into the circuit split between the Second and Seventh Circuits. Agreeing with Second Circuit and disagreeing with the Seventh Circuit, the *Adams* Court has basically adopted expanded definitions of "person" and "entity" under the Act by analyzing the statute's intent and legislative history.²⁴⁸

^{241.} In re: Sealed Case No. 02-001 (United States Foreign Intelligence Surveillance Court of Review) (decided Nov. 18, 2002) WL 31546991.

^{242. 50} U.S.C. § 1803(a) (2000).

^{243.} See FISA, supra note 44 (defining "agent of a foreign power").

^{244.} In re: Sealed Case No. 02-001, supra note 241, at 4.

^{245.} Id. at 33-34.

^{246.} In re: Sealed Case No. 02-001, *supra* note 241, at 18. It can be argued that the court reached its decision to authorize the introduction of evidence obtained prior to the amendment as the court attacks and rejects the primary purpose requirement.

^{247.} USA PATRIOT ACT, supra note 1.

^{248.} Adams, 250 F.3d at 985.

While *Adams* correctly held that government entities may be held liable for violations of the provisions of the Electronic Communications Privacy Act, we certainly have not seen the last of this issue. The circuit split between the Second and Seventh Circuits, as well as the recent reversal of the Foreign Intelligence Surveillance Court decision²⁴⁹ involving the application FISA, leaves many issues open for debate and adjudication. In the wake of September 11, 2001, America's war on Afghanistan, our strong likelihood of war with Iraq, and the new developments in anti-terrorism legislation, there is a strong possibility that the Electronic Communications Privacy Act could be expanded further to include a jump from municipal government liability to federal government liability for violations of the Act.

MICHELLE SCHIPKE SILIES*

^{249.} In re: Sealed Case No. 02-001, supra note 241.

^{*} J.D. candidate 2004, Saint Louis University School of Law; B.S. 1999, Washington University. I would like to thank the editorial board, staff and faculty advisor of the *Saint Louis University Public Law Review* for their invaluable advice and support. Also, a very special thank you to my husband, my precious daughter, and my family and friends for their love, encouragement, and sacrifice during the writing of this comment and the pursuit of my Juris Doctor. This comment is dedicated to those lost in the attacks of September 11, 2001.