Brigham Young University Prelaw Review

Volume 17 Article 7

1-1-2003

The USA Patriot Act and Internet Surveillance

Maren Wells

The USA Patriot Act and Internet Surveillance

Maren Wells[†]

The USA Patriot Act has transformed a pen register from a passive surveillance tool into an intrusive instrument by which government investigators can expose private details of a person's Internet activites before there is probable cause that the person is connected with either criminal or terrorist activites.

Paul Dragomir, manager of the Longshore Motel in Hollywood, Florida, reported that in late August of 2001 two men, now believed to be September 11 hijackers Atta and Ziad Samir, came to his motel and requested a room with 24-hour Internet access. According to Dragomir, these men claimed they were computer engineers from Iran and that they had come from Canada to find jobs. Dragomir put these two men in a hotel room without Internet access while he tried to locate a suitable available room for them. About a half an hour later, Dragomir returned to these two men's temporary room and found two laptops already set-up and waiting for telephone lines to obtain Internet access. Dragomir told the men that he had been unsuccessful in finding a vacant room with Internet access, but that they were welcome to use his office to complete their work. The two men rejected this option and Dragomir apologized for the inconvenience and refunded the men's $175 in cash. Dragomir said at this point the men became angry and one of the guys said, "You don't understand. We are here on a mission." Law enforcement officials later analyzed this need to be online as an indication that the hijackers were looking for Web pages or messages that would signal important information about their developing terrorist plot.[1]

[†] Maren Wells is a freshman from Bountiful, Utah, majoring in political science. After graduation, she plans to attend law school and studying constitutional law.

[1] Farhead Manjoo, "Terrorists Leave Paperless Trail," <http://www.wired.com/news/politics/0,1283,46991-2,00.html>, 28 March 2003.

This incident is a small piece of the mounting evidence that the September 11 terrorists used the Internet extensively to carry out their plot. So far, investigators have discovered that the terrorists used the Internet to book their airline tickets, learn about the aerial application of pesticides, and exchange hundreds of e-mails in English, Arabic, and Urdu containing information about the attack.[2] These discoveries, which illustrate the vital role the Internet played in the September 11 attack, have intensified the debate on appropriate government monitoring of Internet usage. The subsequent results of this debate have manifest themselves in the USA Patriot Act. In this act, the government transforms a pen register from a passive surveillance tool to an instrument which exposes the private details of a person's Internet activities without first having established probable cause. This change to Internet surveillance violates citizens' Fourth Amendment rights as interpreted by past Supreme Court cases and should be amended.

THE USA PATRIOT ACT

On 26 October, less than six weeks after the September 11 attack, Congress passed the USA Patriot Act, which gave the federal government new powers and tools to prevent future terrorist attacks. The formal name of this act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act." This multifaceted and broad piece of legislation includes provisions that grant the government enhanced wire, oral, and electronic communication surveillance tools. Although the Patriot Act quickly passed through Congress with a vote of 357 to 66 in the House and an overwhelming vote of 96 to 1 in

---

[2] Mike Fish, "Numbers Suggest Terrorists Targeted Flights," CNN News, <http://www.cnn.com/2001/US/09/19/hijacked.planes/>, 28 March 2003; P. G. Madrinan, "Eighteenth Century Papers in Twenty-First Century Drawers: After September 11, Do the Websites You Visit on the Internet Deserve Fourth Amendment Protection?" *Search and Seizure Law Report* 54 (June 2002): 36; "The Proof They Did Not Reveal," *Sunday Times*, 7 October 2001, <http://www.unansweredquestions.net/timeline/2001/sundaytimes100701.html>, 28 March 2003.

the Senate, some of this act's controversial provisions have become part of a nationwide effort balance national security and civil liberties in an unsure atmosphere.[3]

Background

For decades the Supreme Court has struggled to balance an individual's constitutional right to be secure against unreasonable searches and seizures and law enforcement's need to use electronic surveillance technology for domestic and national protection. In 1928 the Supreme Court first ruled whether the government's use of a technology to monitor communication offended the Fourth Amendment's ban against searches without a warrant. In this case, *Olmstead v. United States*, the Supreme Court ruled in a five to four decision that the government's use of wiretapping without a search warrant did not violate the suspect's Fourth Amendment right because there had been no physical intrusion of the property where the calls were made.[4]

Thirty-nine years after the *Olmstead v. United States* case, the Supreme Court faced another electronic surveillance controversy. In *Katz v. United States*, FBI agents had tapped a public telephone booth without obtaining a warrant. In their decision, the Supreme Court overturned the ruling in the *Olmstead* case. Justice Stewart wrote the majority opinion stating that the Fourth Amendment protects an individual's "property and privacy."[5]

The legislative response to the Supreme Court's decision in *Katz v. United States* was Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III established that law enforcement agents could use wiretapping as a surveillance tool for criminal investigative purposes if a judge identifies a probable cause that a serious

---

[3] Steven Osher, "Privacy, Computers and the Patriot Act: The Fourth Amendment Isn't Dead, But No One Will Insure It," *Florida Law Review* 54 (2002): 522.

[4] T. Gardener, *Principles and Cases of the Law of Arrest, Search, and Seizure* (New York: McGraw-Hill Book Company, 1974): 354. Wiretapping is defined as "eavesdropping and overhearing telephone conversations."

[5] *Katz v. United States*, 389 U.S. 347 (1967).

crime has been, is being, or will be committed.[6] If probable cause exists, the judge will give the federal agents a warrant permitting wiretapping. Only in emergency situations, which include immediate danger of death or serious injury to any person or conspiratorial activities characteristic of organized crime, may law enforcement officers engage in wiretapping without a warrant. In such situations, an application for a warrant must be made within forty-eight hours after wiretapping has occurred.[7]

Title III also deals with pen registers. Pen registers are similar to caller ID devices: they record the date, time, and telephone numbers of outgoing and incoming calls, but not the content of the telephone call.[8] Because of the less intrusive nature of the pen register, probable cause of criminal activity is not required for law enforcement officials to obtain a warrant from a judge in order to install a pen register. Nonetheless, domestic law enforcement government officials seeking to install a pen register must certify to a court that "the information likely to be gathered is relevant to an ongoing criminal investigation being conducted by that agency."[9]

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 limits electronic surveillance in domestic investigations, but it does not limit the executive branch's surveillance authority. Ten years after Title III, Congress enacted the Foreign Intelligence Surveillance Act of 1978 (FISA), which defines the extent to which the government can engage in wiretapping for national security purposes. Under FISA, a federal officer must make each application for surveillance authority. This federal officer must have the

---

[6] 407 U.S. at 316. The importance of probable cause in order to legally wiretap a phone was stressed later in *United States District Court v. United States* when the Supreme Court stated that the "very heart of the Fourth Amendment directive: that, where practical, a governmental search and seizure should represent both the efforts of the officer to gather evidence of wrongful acts and the judgment of the magistrate that the collected evidence is sufficient to justify invasion of a citizen's private . . . conversation."

[7] Sharon Rackow, "How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of 'Intelligence' Investigations," *University of Pennsylvania Law Review* 150 (2002): 1659.

[8] Michael McCarthy, "USA Patriot Act," *Harvard Journal on Legislation* 39 (2002): 443.

[9] 18 U.S.C. § 3122(b)(2) (2001).

application approved by the Attorney General and then present it to the Foreign Intelligence Surveillance Court, which consists of seven district court judges appointed by the Chief Justice of the United States.[10] Unlike Title III, the members of the Foreign Intelligence Surveillance Court can grant a warrant for wiretapping without probable cause of a crime. Instead, the federal officer simply has to show probable cause, that the primary purpose of the surveillance is intelligence gathering, and that the suspect being wiretapped is a foreign power or an agent of a foreign power.[11] This process provides much broader electronic surveillance capability for gathering foreign and national security intelligence than for criminal investigations.

FISA also deals with the use of pen registers for the purpose of gathering foreign and national security intelligence. Under FISA an agency seeking permission to install a pen register to monitor a suspect's telephone, must certify that the pen register is likely to provide information relevant to a foreign surveillance investigation. Again the FISA requirements to obtain a pen register are far less stringent than the requirements needed to gain a warrant to engage in a wiretap, because the wiretap allows law enforcement officials to listen to the suspect's conversations.[12]

A third major Supreme Court decision that has preceded the USA Patriot Act is *Smith v. Maryland.* In this case, the Supreme Court's ruling on the use of pen registers decided that "a person has no legitimate expectation to privacy in information he voluntarily turns over to third parties."[13] In other words, a person placing a telephone call does not have a reasonable expectation of privacy because the number he or she dials is relayed to a telephone company's central office. Those who use the telephone risk that the phone company might give this information to the government. Because of

---

[10] Jennifer Evans, "Hijacking Civil Liberties: The USA Patriot Act of 2001," *Loyola University Chicago Law Journal* 33 (2002): 955.

[11] Ibid.

[12] Ibid.

[13] *Smith v. Maryland*, 442 U.S. 735 (1979).

this assumed risk, the Court found that no unreasonable search had occurred and upheld Title III and FISA legislation about using pen registers without first establishing probable cause.

CHANGES TO INTERNET SURVEILLANCE BY THE USA PATRIOT ACT

Section 216 of the USA Patriot Act allows a pen register to be used on devices that track "dialing, routing, addressing, or signaling information."[14] This change means that a pen register can be used for tracking e-mail and Internet usage in addition to telephone calls. A pen register that monitors a suspect's Internet usage allows law enforcement officials to obtain such information as visited Web addresses and e-mail addresses of the suspect's incoming and outgoing e-mail. The law enforcement officials can obtain permission to use a pen register to monitor a suspect's e-mail and Internet usage the same way they are able to obtain permission to use a pen register on a suspect's telephone: obtaining certification from a government attorney or investigative officer that the information likely to be gathered is relevant to an ongoing criminal or foreign intelligence investigation.[15]

The use of a pen register as a tool for Internet surveillance is problematic, primarily because its function is very different from a pen register used to monitor telephone activity. For example, when a person makes a telephone call, the content of the communication is separable from the transactional data used to connect with another phone. Unlike a phone, the Internet functions by using a technology known as packet switching. This technology breaks data down into small packets of information, which are transmitted and then reassembled, in the correct order at the designated computer. This type of technology doesn't allow a pen register to separate the transactional data from the content of the exchanged information. For example, a law enforcement agency using a pen register to monitor a suspect's e-mail usage would receive both the transactional data and the contents of the suspect's e-mail. The agency would then

---

[14] 18 U.S.C §§ 3123(a)(3)(A) (2001).

[15] Ibid.

have to be trusted to save the e-mail addresses and discard the contents of the e-mail.[16] This implies that this law enforcement agency would be able to refrain from investigating the contents of the email. According to Justice Douglas, this implication of restraint, especially in a situation where lives may be endangered is not only idealistic, but constitutionally erroneous.[17]

Even if the content of the email is properly separated by a third party to ensure that the investigators receive only the Web and e-mail addresses recorded by the pen register, other problems still exist. For example, by re-entering a Web address there is a strong possibility that an investigator can locate the exact information previously displayed on the suspect's computer. This is unlike monitoring telephone calls because an investigator cannot redial the telephone number captured by a pen register and listen to a previous conversation or even obtain the topic of that conversation. Because of this discrepancy, the critics claim that the World Wide Web is much more like a library than a phone. The ACLU has declared that using a pen register to monitor Internet usage is comparable to having a librarian report to government agents what "books [a suspect] perused while visiting the public library."[18] If libraries require law enforcement agents in most states to have probable cause to obtain a warrant to see records related to the circulation of library materials that reveal personally identifying details of library patrons, why should situations involving the Internet abide by less protective measures?

Conclusion

The lack of proof required to use a pen register to monitor a suspect's Internet usage is a threat to citizens' Fourth Amendment rights. The USA Patriot Act has transformed a pen register from a passive surveillance tool into an intrusive instrument by which government investigators can expose the private details of a person's Internet

---

[16] Ibid.

[17] *Katz v. United States*, 389 U.S. 347 (1967) (Justice Douglas, concurring opinion).

[18] Ibid.

activities before there is probable cause that the person is connected with either criminal or terrorist activities. The government also does not need the added surveillance powers granted in the USA Patriot Act, because it already has sufficient means to investigate criminal activities and gather intelligence information necessary to safeguard national security through Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and FISA. Section 216 of the USA Patriot Act should be amended so a pen register can be used to monitor Internet use only after probable cause has been established because Internet technology does not make a pen register the simple caller ID tool that it is for a telephone. If section 216 of the USA Patriot Act is not amended then the United States is allowing the Fourth Amendment rights of more than fifty million U.S. households that are online to be eroded to obtain a greater sense of false security.[19] American citizens must remember Senator Russ Feingold's statement that "there have been periods in our nation's history when civil liberties have taken a back seat to what appeared at the time to be legitimate exigencies of war . . . We must not allow this piece of our past to become prologue. Preserving our freedom is the reason that we are now engaged in this new war on terrorism. We will lose that war without a shot being fired if we sacrifice the liberties of the American people in the belief that by doing so we will stop the terrorist."[20]

[19] John Podesta, "USA Patriot Act: The Good, the Bad, and the Sunset," *Human Rights* (Winter 2002): 3.

[20] Peter Del Bianco, "The Case for Civil Liberties," *Maine Bar Journal* (Winter 2002): 21.