Legal Times
WEEK OF SEPTEMBER 26, 2005 • VOL. XXVIII, NO. 39
ALM

They're Listening

Because of a Fourth Amendment loophole, government can spy on international calls by U.S. citizens.

BY JOSEPH A. HENNESSEY

The Fourth Amendment faces a new threat—outsourcing. As American jobs move offshore, American privacy rights are leaving with them, opening a loophole that, in effect, lets law enforcement agencies spy on American citizens without search warrants.

Government encroachment on privacy begins where the Fourth Amendment protection ends—at the border of the United States. The act of placing an international telephone call causes one to "leave" the United States and its protection against unreasonable government intrusions on privacy.

Lawyers who make international calls should know that such calls are unprotected by the Fourth Amendment and can be (and generally are) intercepted by the U.S. government. Yet what of the outsourced calls that are routed, without a consumer's consent, to overseas call centers located in such places as India and Pakistan? Those calls, also, can be (and generally are) intercepted by the U.S. government. The government's intrusion into the privacy of calls that are routed to overseas call centers further erodes the protection of the Fourth Amendment.

A recent example of the constitutional threat arose from something as unremarkable as calling for help with a computer problem. My subscription to an anti-virus program expired. I called the software company's "800" number when I encountered difficulty in reactivating the service. Since I neither dialed "011" to access an international number nor asked for the assistance of an overseas customer service agent, I had the reasonable expectation that the number I had dialed would be answered in the United States.

Yet the gentleman who answered my call was not an American citizen. (I asked when I heard his accent). Only when I pressed him did he reveal that he was fielding my call from India. He then asked for and obtained my e-mail address, credit card number, purchase order, and confirmation number.

This sort of outsourcing is not at all unusual, and it is increasing. *Time* magazine reports that banks, insurance companies, and mortgage lenders are following the technology sector in outsourcing operations. The magazine estimates that in the next five years, more than 500,000 financial services jobs will be sent to offshore service centers. Here, employees will assist customers with confidential data such as mortgage applications, financial investments, and estate planning.

Yet American citizens participating in conversations with such overseas service centers may not realize some troubling facts: Their telephone calls, frequently routed overseas without their consent, are not protected under the Fourth Amendment, and their government is listening.

NO WARRANTS

U.S. citizens have the protection of the Fourth Amendment to safeguard them against unreasonable government invasions of their privacy. This amendment establishes that "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."

Generally speaking, a search warrant will not be issued by a court unless the government demonstrates that probable cause exists to believe that the search will reveal evidence of a crime. Our society has recognized the reasonable expectation of the privacy in telecommunications by codifying, at 18 U.S.C. §2511(1)(a), a prohibition against intentionally intercepting "any wire, oral, or electronic communication."

The Fourth Amendment, however, has territorial limits. In *United States v. Verdugo-Urquidez* (1990), the Supreme Court made clear

that Fourth Amendment protections are enjoyed only by "the people" of the United States and do not apply to non-U.S. citizens residing overseas.

Since the Fourth Amendment provides no protection to foreigners living overseas, the National Security Agency has the authority to intercept any communication that has at least one foreign terminus. The same statute that makes it a criminal act to intercept wire, oral, and electronic communications preserves the NSA's right to intercept such signals when they are directed outside the United States.

In fact, the NSA does intercept and seize almost all international telecommunications through an eavesdropping network known as Echelon. Echelon is a satellite-based interception system operated by the intelligence agencies of the United States, the United Kingdom, New Zealand, Australia, and Canada. As reported by Erin Brown in a 2003 law review article, Echelon intercepts as many as 3 billion electronic communications every day. The memory buffers maintained by the NSA are thought to be capable of storing 5 trillion pages of this captured data.

Captured raw data are digitally searched using key words and phrases supplied by the intelligence agencies of the five participating countries. If the big ears of Echelon capture a designated key word or phrase in a communication, that "hit" is reviewed by an intelligence analyst.

By the nature of the Echelon system, the telephone conversations that contain hits can be provided not only to the U.S. government but possibly the governments of Australia, New Zealand, the United Kingdom, and Canada. Thus, when you make that phone call overseas, a lot of ears could be listening.

FOR BOLTON'S EYES

The NSA is under no legal obligation to safeguard the privacy of communications where the foreign terminus of the call places such communications outside the protection of the Fourth Amendment.

During the confirmation hearings of John Bolton as the U.S. representative to the United Nations, it came to light that the NSA had freely revealed intercepted conversations of U.S. citizens to Bolton while he served at the State Department. (The president has since given Bolton a recess appointment to the U.N. job.) More generally, *Newsweek* reports that from January 2004 to May 2005, the NSA supplied intercepts and names of 10,000 U.S. citizens to policy-makers at many departments, other U.S. intelligence services, and law enforcement agencies.

Surprisingly, the legality of the NSA transferring intercepts to other branches of the federal government appears to be a closed question in the eyes of the courts, at least with regard to the Fourth Amendment.

In *Jabara v. Webster* (1982), the U.S. Court of Appeals for the 6th Circuit established that once information—any information—is lawfully in the possession of the NSA (which it is any time there is at least one overseas terminus to a telephone call), there is nothing improper about the NSA transferring the intercepted information to another branch of the federal government.

In *Jabara,* the NSA had intercepted calls from a Detroit-based attorney that terminated overseas. The 6th Circuit ruled that once the NSA "lawfully" intercepted those communications, there was no obstacle to transferring the captured information to the Federal Bureau of Investigation. The FBI received and used the intercepted telephone conversations though it had not, itself, applied for a wiretap or search warrant from a court.

The 6th Circuit acknowledged that the attorney had an actual (subjective) expectation of privacy when he sent the messages overseas. But it questioned whether society was "prepared" to recognize the expectation as reasonable after the NSA obtained the messages. Ultimately, the court asserted that "We do not believe that an expectation that information lawfully in the possession of a government agency will not be disseminated, without a warrant, to another government agency is an expectation that society is prepared to recognize as reasonable."

RECLAIMING LIBERTY

Because of job losses, American citizens are becoming increasingly cognizant of outsourcing. In reaction, many overseas call operators are under strict instructions to make the customer believe that the call is being handled in the United States.

The labor union Communications Workers of America,with the support of allies in Congress, has been pushing to put an end to such ploys. The Call Center Consumer's Right to Know Act, introduced by Sen. John Kerry (D-Mass.) and Rep. Ted Strickland (D-Ohio), would require U.S. companies to disclose the physical location of the call center at the beginning of each call. Ironically, Sen. Bill Frist (R-Tenn.) criticized this bill as placing the country on a "path of more Government . . . with less freedom."

Yet the disclosure that a customer's call is being fielded offshore would not only alert a consumer to the existence of an outsourced job, it could also provide the prompt needed for American citizens to safeguard their Fourth Amendment rights. Those wishing to ensure the privacy of their telephone communications could insist on a U.S.-based telephone operator.

Beyond this, ideally, Congress should bar the NSA from revealing the intercepted identities of U.S. citizens to other branches of the federal government, except where there exists a significant, clearly established risk to national security. An imminent terrorist attack would qualify, but routine law enforcement—let alone mere curiosity—should not.

Congress is also free to disagree with the 6th Circuit's conclusion in *Jabara*. Specifically, Congress could require law enforcement to apply to a court and demonstrate probable cause before obtaining NSA intercepts of conversations involving targets of a criminal investigation. Congress could bar the use of NSA intercepts in criminal prosecutions where domestic law enforcers have not convinced a court beforehand that a review of NSA intercepts will reveal evidence of a crime. Such safeguards could prevent law enforcement from engaging in fishing expeditions by casting lines in the pool of intercepted overseas calls.

Congress and the federal courts need to be more vigilant about protecting U.S. citizens from these abuses. As the Supreme Court recognized in *Katz v. United States* (1967), the Fourth Amendment protects people, not places.

Though the economy might be globalized, the U.S. Constitution is not. Its protections should not be so casually set aside.

Joseph A. Hennessey is a partner in Newman, McIntosh & Hennessey, located in Bethesda, Md. He can be reached at jhennessey@nmhlaw.com.